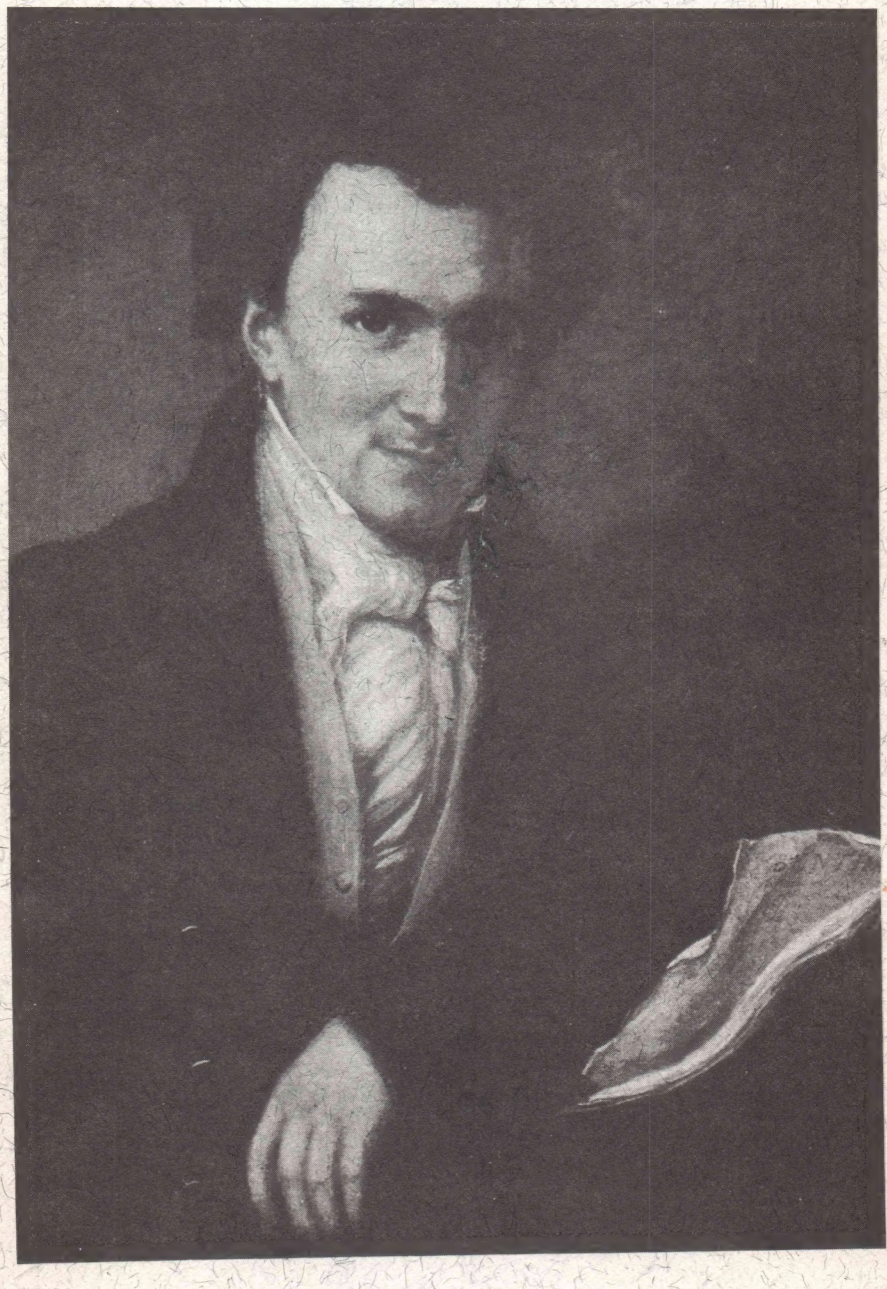
A Quarterly Journal Devoted to All Aspects of Cryptology

CRYPTOLOGIA

Volume 7 Number 4 October 1983



CRYPTOLOGIA

A Quarterly Journal Devoted to All Aspects of Cryptology

All correspondence concerning subscriptions, advertising and publications should be sent to the publisher at the Editorial Office, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

See inside back cover for subscription information.

ISSN 0161 - 1194. Manufactured in the United States of America.

Cover: Who was Nicholas Trist and what search by scholars did he cause? (See article on page 297.)

Assistance of Rose-Hulman Institute of Technology is acknowledged and appreciated.

LETTER FROM THE EDITOR

CRYPTOLOGIA began as an idea in the head of C. A. Deavours, one of our current editors, an idea for a newsletter for those who were teaching cryptology courses in colleges and universities. In 1976 at the National Computer Conference in New York City five people met to discuss this idea: C. A. Deavours, David Kahn, Louis Kruh, Greg Mellen, and myself, Brian J. Winkel. We had a good discussion about how we might proceed and what the journal would feature. I was volunteering to do the final production of the journal and I was talking to publishers about our new idea, which had not really received a name as yet. We had a few dozen interested subscribers and when I approached the publishers they wanted to know how many thousands we had in line! I was thinking hundreds - maybe! I returned home not knowing how to approach the organizing, managing editing, or publishing of this new journal, CRYPTOLOGIA.

There in my pile of mail was a small envelope with a catalog of material published by an Aegean Park Press, P O BOX 2837, Laguna Hills CA 92653. This group was publishing and apparently profiting from the sale of old (World War I and II) cryptologic material, official declassified government manuals, non-governmental material and some unpublished material. If these fellows thought they could make money off such material surely they might consider publishing a journal with both current and historical material.

After a fews calls to Wayne Barker, the publisher at Aegean Park Press, we began to prepare material for camera-ready offset shooting by the Press and Wayne agreed to print the journals without upfront payment, but rather to risk waiting for subscriptions to recover his costs and profits. So with a combination of material prepared on a borrowed Physics Department Selectric typewriter and the press' typewriter we sent out our first issue in January 1977. We worked for two years with the Press. Then, because we felt we were well enough established in procedure, content and subscription base, and because Aegean Park Press is primarily a book publisher, not a periodicals publisher, we went to a reputable press in Michigan, Cushing-Malloy Lithographers of Ann Arbor (they do the Mathematical Reviews and other fine journals) and we still work with them after producing camera-ready copy. Currently we use a NEC Spinwriter printer, driven by WordStar word processing software on an Ohio Scientific Instruments computer under a CP/M operating system. We find that this permits editing and corrections as are necessary and gives quite satisfactory camera-ready copy.

That is our past. Our present involves you, the reader, and we should like to know what you think of our work and how we can better serve you. Please take the time to fill in the comments space on the enclosed renewal form - even if

you are not renewing your subscription with this issue. Let us know what you want to see in the journal, what you think about our coverage so far, and what you believe we should do to improve our work.

Final word: Below is an announcement about our Undergraduate Paper Competition. In its first year we had an excellent paper for a winner and last year we had no entries. Please consider urging some undergraduate to submit a paper for the competition. Papers exist in this area, we know, and students need to be encouraged to submit them to competitions. Thank you.

Cryptologia Third Annual
Undergraduate Paper Competition
in Cryptology

We announce this contest to encourage the study of all aspects of cryptology in the undergraduate curricula.

FIRST PRIZE: Three hundred dollars

Closing date: 1 January 1984

Paper topic may be in any area of cryptology technical, historical, or literary subjects.

Papers must be no more than 20 typewritten pages in length, double spaced and fully referenced. Four copies must be submitted. Authors should keep one copy. Papers are to be original works which have not been published previously.

The papers will be judged by the Cryptologia editors and the winner will be announced on 1 April 1984 with publication of the winning paper in the July 1984 issue of Cryptologia.

The competition is underwritten by a generous gift from Boshra H. Makar, Professor of Mathematics, Saint Peter's College, Jersey City New Jersey.

Inquires, submissions and subscription information:

Cryptologia
Rose Hulman Institute of Technology
Terre Haute, Indiana 47803

HOW TO USE THE GERMAN ENIGMA CIPHER MACHINE
A PHOTOGRAPHIC ESSAY

LOUIS KRUH

What follows is a step by step procedure for using the German Enigma machine. This machine is an authentic Enigma machine and has been used effectively as an aid to teaching cryptology at Kean College of New Jersey and Rose-Hulman Institute of Technology.

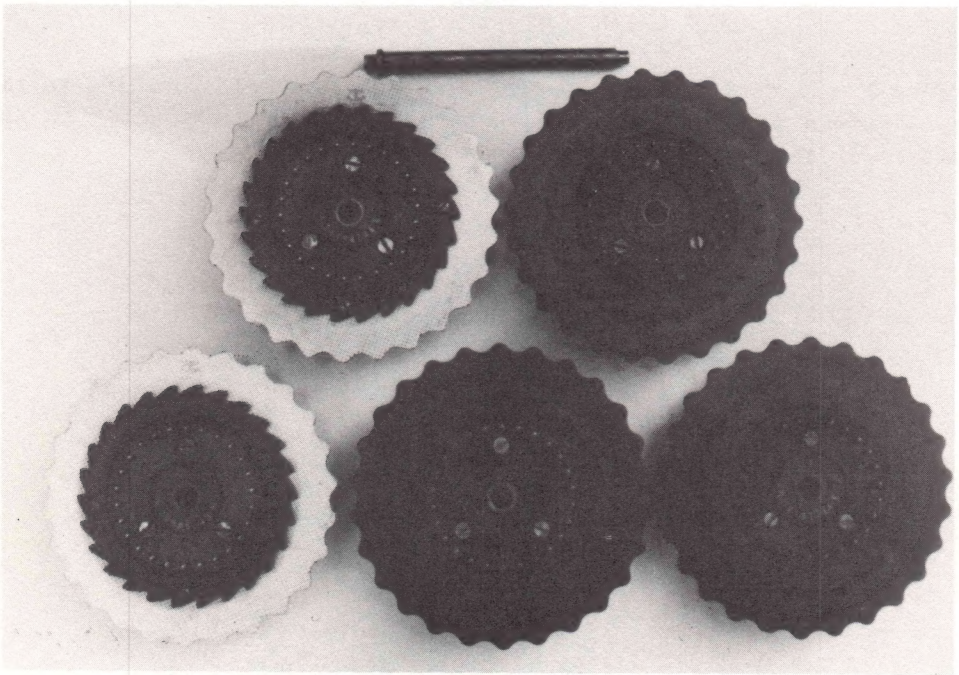


Figure 1. Step one is to choose three rotors from the five that are available and arrange their sequence from left to right. (They are numbered I, II, III, IV and V.)

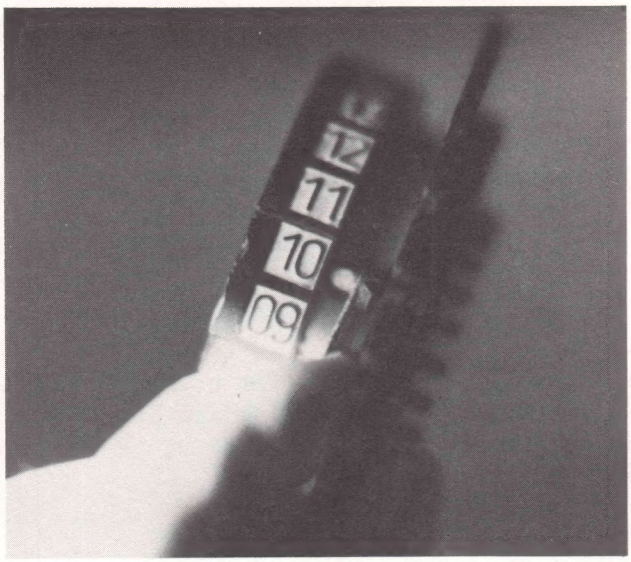


Figure 2. Then the number ring of each rotor is set according to the key. Rotors were marked with numbers 1 - 26, corresponding to the letters of the alphabet.

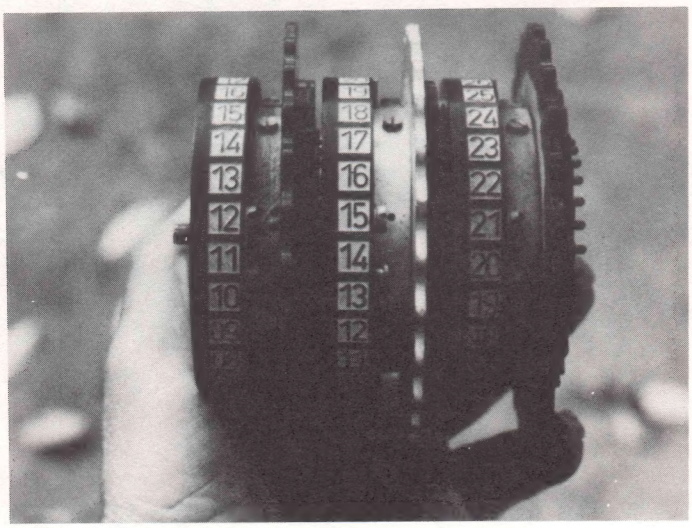


Figure 3. The rotors are assembled on their shaft.

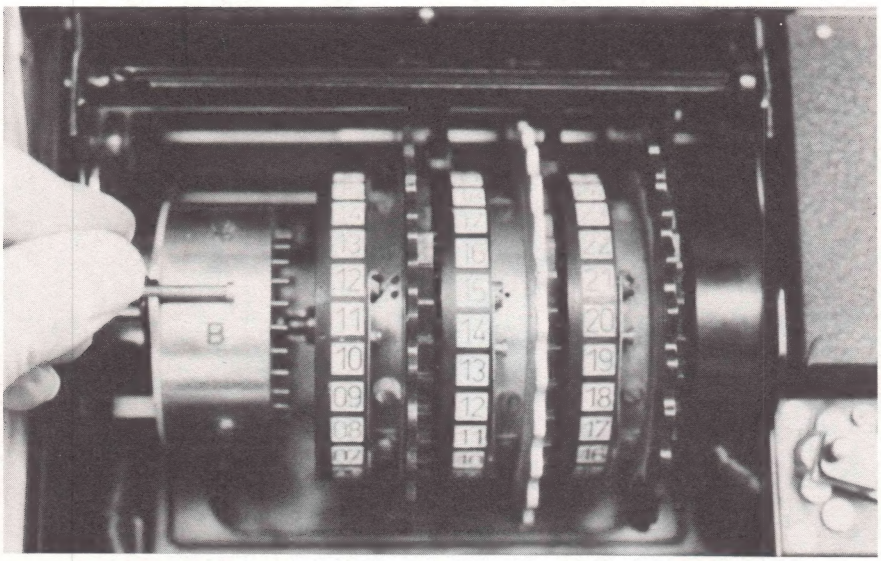


Figure 4. After the rotors are inserted moving the lever to the rear forces the non-removable reflecting rotor and the other rotors into contact with each other.

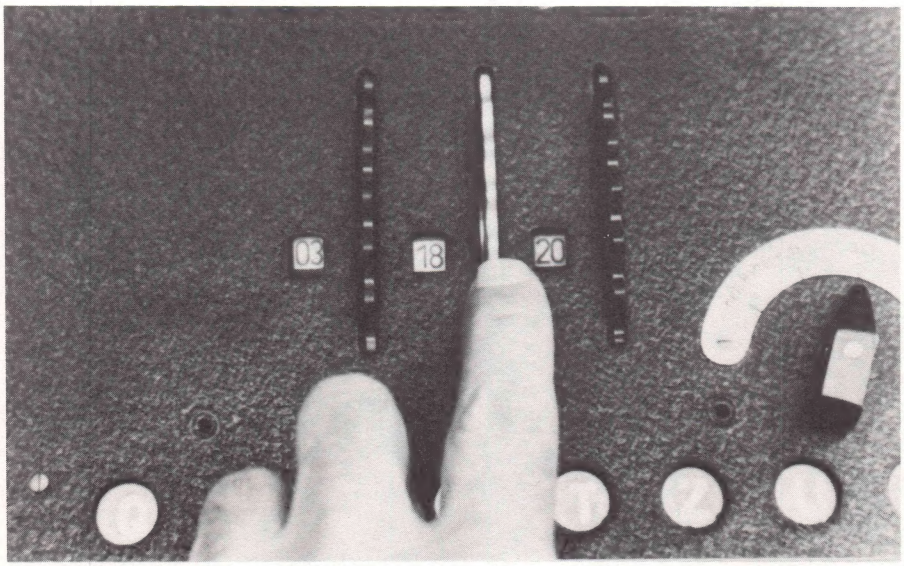


Figure 5. One by one the individual rotors are rotated to arrange their initial or primary settings in the three windows.

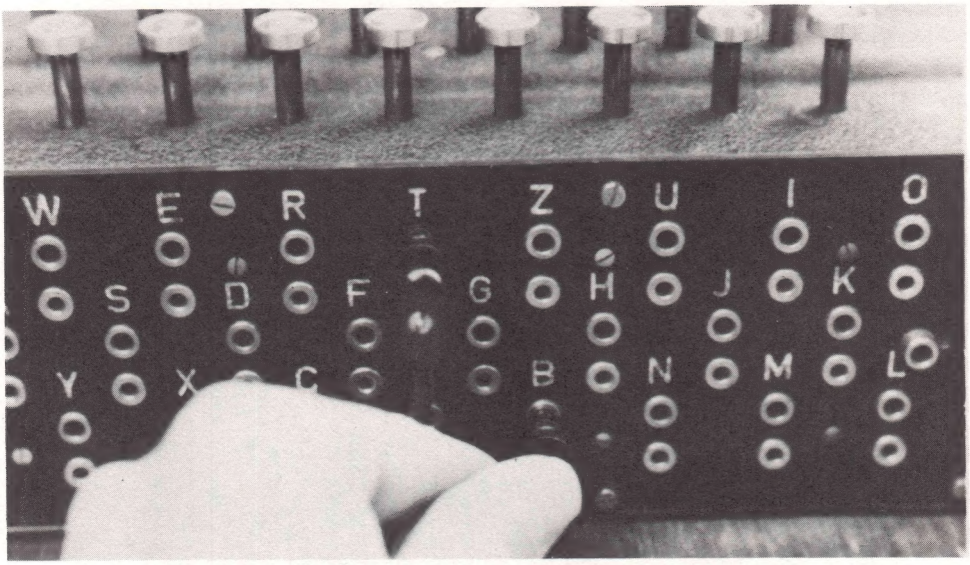


Figure 6. The final settings are the patch cord connections. Here the first connection from T to B is being completed with the double patch cord.

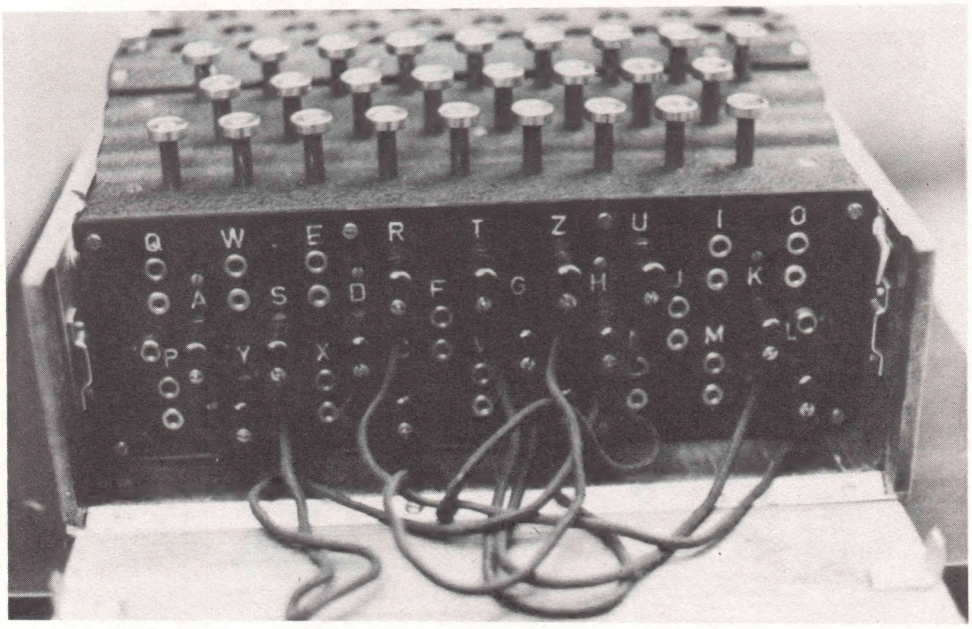


Figure 7. A close-up of the patch board with seven double plugs inserted.

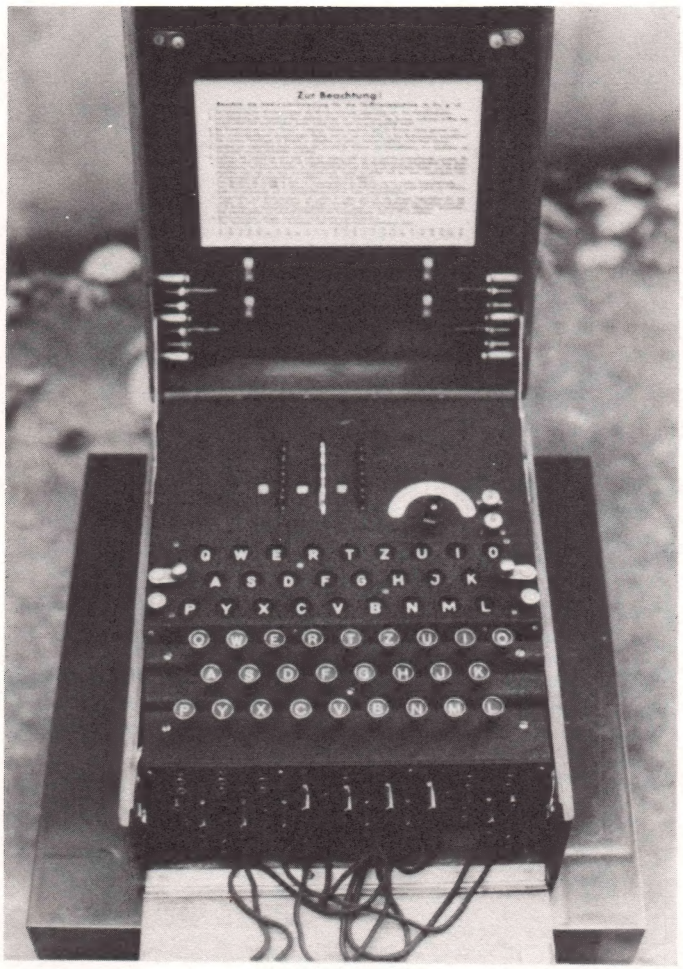


Figure 8. The setting of the keys is finished and the Enigma is ready to use.

This description omits procedures for establishing and/or transmitting key setting information to recipients of enciphered messages. It was, incidentally, the sending of that information by the Germans that enabled Polish cryptanalysts to find an entry into the cipher that ultimately led to its solution.

In military units daily key list information would be provided on a monthly basis. Following is how the key information used in our example above might appear for the 29th day of the month.

Date	Rotor Sequence	Ring Settings	Primary Settings	Patch Cord Connections
29	IV I II	12 15 21	03 18 05	TB GK LR HU DH YS CZ

After preparing the key settings the cipher clerk types each letter of the cleartext. As each letter is depressed, a letter lights up, which is the ciphertext. Following is a message enciphered with the above keys for those wishing to try their cryptanalytic skills or use their own Enigma to decipher the text. Instructions for the Enigma warn the user not to encipher messages longer than 180 letters. This message contains 205 letters. Good luck.

YJXSI DJWLS BWJOW VBDLY YNLHL SRZOD MHIXM GGGWE BLQPT RRMRJ

EQHZQ NADAD OQCLS MGOHS VMZKC LHMAK XYWXJ HRYCH FITRS LZJIN

LAHFN HGVMF QWHKO SBXLT XHSMM JLBXC GFQHZ GYMTB QPWVW VJICX

XMDTE HRWFJ BKCXI RJDHN WGIGH EVRWA OBDPG HSBGZ MLKHB KTGNC

FQANZ

THE SEARCH FOR THE KEY BOOK TO NICHOLAS TRIST'S BOOK CIPHERS

ALBERT C. LEIGHTON AND STEPHEN M. MATYAS

The name of Nicholas Philip Trist is known to few Americans even though he negotiated a treaty which brought to the United States one of its greatest territorial accessions—the entire Southwest--after the 1848 victory over Mexico. Furthermore, he did this after having been disavowed and recalled from his position as special envoy to Mexico by the President of the United States. Sent to Mexico without secure means of communication, he was forced to devise methods of encipherment which he could use to inform Washington of his actions. This article will explain the bases of his ciphers and reveal hitherto unknown information about them.

Figure 1. Nicholas P. Trist at an Early Age (from the Collection of Mrs. Gordon Trist Burke).

The life of Nicholas Trist can be briefly sketched. He was born in Charlottesville, Virginia, in 1800. His grandmother had been an old flame of Thomas Jefferson. As a consequence, the families were friendly and Nicholas spent time at Monticello where he eventually married Jefferson's favorite granddaughter, Virginia Randolph, uncharitably described by Trist's mother as a tall girl of "not great personal charms."[1] Trist himself was a slender, unhealthy six feet weighing only 120 pounds (Figure 1). At Monticello he became the favorite companion of the aging ex-president and was present at Jefferson's deathbed in 1826, informing him that he had achieved his goal of surviving until the Fourth of July. As executor of Jefferson's will, he had the difficult task of dealing with Jefferson's confused finances and administering Monticello. After unsuccessful attempts at practicing law and running a newspaper, he eventually obtained a position as clerk in the State Department by political patronage, primarily because of his Jeffersonian connections. His position was continued into the administration of Andrew Jackson where, once more because of personal relationships, he also acted as private secretary to the president.[2] Later made consul at Havana, for which he seemed well suited because of his knowledge of Spanish, he irritated many and had a difficult time. His reports and letters were characterized by extreme verbosity. It was said "Of wit he had none, if brevity be its measure" and his "written explanations from Havana were too prolix for comprehension."[3] By 1845 Trist was back in the State Department as chief clerk (which, under the conditions of the time, meant that he was next in authority to his friend James Buchanan, the new secretary of state and the future president).

When the Mexican War came, Generals Zachary Taylor ("Old Rough and Ready") and Winfield Scott ("Old Fuss and Feathers") were both successful and both Whigs. The president, James K. Polk, was a Democrat and not eager for them to achieve great fame and become his potential political rivals. Not wanting these commanders in the field to gather additional laurels by negotiating the peace treaty, he selected Nicholas Trist as his personal representative to go secretly to Mexico with instructions and a draft treaty to present to the Mexican government. A hint was even given of a "possible nomination to the presidency in the event of his success."[4] Trist attempted to travel incognito but his cover was soon blown and accounts of his "secret" mission were published in the newspapers. So were the seeds of distrust planted. Infuriated, Polk blamed both Trist and Secretary of State Buchanan for the leak.

Trist's arrival in Mexico was no more auspicious. Through ineptness, he quarreled with Scott, but after Scott later sent a gift of guava jelly to the sick Trist, they became fast, life-long friends. In the chaotic situation in Mexico, Trist had difficulty in finding any effectual Mexican government with which to negotiate.

Trist's Ciphers

Trist soon realized he had no secure means of communication with Washington. Consequently, he devised two ciphers which he described in two letters to Buchanan.[5] The first system is described in his letter of June 3, 1847, pertinent parts of which are here excerpted:

Puebla, June 3, 1847

James Buchanan
Secretary of State

*... I have been occupying part of my time here in making a cipher, which I shall probably have frequent occasion for. A duplicate and key can be made at the Department by sending to my daughter for a copy of the smallest of the books (there are several at my house) which she packed up for me: The work of our old instructor, who was sent to Spain as Consul. Let the letters of the prefatory address "To the British Nation" (excluding this title) be numbered, from one onward until every letter of the alphabet is reached, except Z (which I represent by zero). Each of the letters, with a few exceptions has three numbers corresponding to it.

Nicholas P. Trist

In a postscript to his dispatch No. 9 of July 23, 1847, he repeats the description of the first type of cipher and adds a description of his second encipherment method. He later called this "treble numbered" and planned to use it for particularly important passages. The pertinent parts of the P.S. are here excerpted:

Puebla, July 23, 1847

Hon: James Buchanan
Secretary of State

*....
P.S. July 25
I have already given the Key to the cypher here used. Lest, however, my letter may have miscarried, I will here repeat it. Send to my house for a copy (there are several) of the smallest of the books which my daughter packed in my trunk—the work of our old instructor at Washington. Number the letters of the address "To the British Nation" (omitting this title) and you have the key.

In future, I will, for passages of special consequences vary the cypher as follows. Three numbers between brackets will indicate the page, the line and the letter. The same book "Part Second," to be used. If there be more than three numbers within the same brackets, all after the third will indicate letters in the same line. For example: (33,4,5) will indicate the letter g.

Nicholas P. Trist

The principle of the first method is that used by Charles William Frederic Dumas and Benjamin Franklin in 1776[6] and by the originator of the Beale ciphers in 1822, where the letters of a selected text are numbered serially, thereby furnishing several equivalents for each letter of the alphabet.[7] Such a system is difficult to decipher without the key text. Trist's second method of encipherment is similar to that used by Benedict Arnold and British Major John André in their treasonous correspondence in 1779[8] and to the Thurn-Taxis cipher used in Bavaria in the early 1800's.[9] Such ciphers were described and may have been popularized by Johann Ludwig Klüber in his book Kryptographik published in 1809 in Tübingen.

0 z	14 c,e	28 f	45 n	114 p
1 t	15 i	29 t	50 r	115 y
2 h	16 g	30 e	52 w	121 m
3 e	17 n	31 r	58 d	133 p
4 s	18 1	33 h	59 i	147 t
5 t	19 a	34 i	61 b	167 w
6 u	20 n	35 m	64 d	183 p
7 d	21 g	36 c	65 1	196 m
8 y	22 u	37 q	73 h	200 v,1
9 o	23 a	38 u	99 b	215 b
10 f	24 g	39 i	100 1	300 x
11 f	25 e	40 s	102 w	409 k
12 o	26 s	41 i	105 c	448 v
13 r	27 a	44 o	110 f	

Figure 2. Trist's Cipher Key Recovered from State Department Despatches.

Several scholars have written of Trist, but most of them have had little interest in his ciphers.[10] (Robert Arthur Brent's 1950 Ph.D. dissertation "Nicholas Philip Trist: Biography of a Disobedient Diplomat" at the University of Virginia does not mention Trist's ciphers.) However, Ralph E. Weber, professor of history at Marquette University and author of United States Diplomatic Codes and Ciphers was able to reconstruct much of the key to

Trist's first method by consulting official State Department decipherments. [11] From these decipherments, Weber determined that Trist's key text began with the words "The study of foreign languages after...." (Figure 2). But Weber did not identify Trist's key book, which would have been necessary to complete the key and unlock those dispatches which used Trist's second method.

In Trist's slow and tortuous negotiations with the almost nonexistent Mexican government, he was considerably aided by the British diplomats in Mexico, particularly Edward Thornton (later to be Sir Edward Thornton, British ambassador in Washington for many years). In fact, it appears from a private letter to Buchanan attached to Trist's dispatch No. 10 of July 31, 1847, that Thornton was the originator of Trist's treble numbered cipher:[12]

Puebla, July 31, '47

Private.
Hon: James Buchanan
Secretary of State.

Sir,

To my No. 10 of this date I will here add, that my engagements are becoming quite laborious—such as would be so, even if I were in vigorous health and in a different climate. Yesterday, for instance, I was closely engaged from 12 o'clock till dusk, in what ought to have been the employment of a confidential assistant: putting in cypher (a treble numbered cypher selected by him) a short note to 121,13,1,2,17,5,9,20. It was to be ready by three o'clock, but this proved impracticable. Fortunately, however, the courier-spy (as these men may be called) was accidentally delayed, so that I did not miss the opportunity. Everybody—generals and lieutenants—expresses great surprise at my not having "a secretary"; and independently of any interest I might have had in the question, I think it unfortunate, in more important respects than that of my being a little overworked, that this mission was not made a full one, as all seem to take for granted that it is. Genl. Scott has offered me assistance from the army; and although I have not yet, for various reasons, availed myself of it, I shall do so, to keep up appearances with the Mexican Commn., should there be a meeting.

I am, Sir, very respectfully
Yr observt
N. P. Trist.

His identity is revealed by applying Weber's reconstructed key to the cipher text above:

```
  m  r   th  n t o  n
121,13,  1,2,17,5,9,20
```

Despite his mistakes in enciphering, it is apparent that Trist intended to write "Mr. Th[or]nton."

Communications between Washington and Trist were extremely slow. For example, Trist's dispatch No. 9, sent on 23 July 1847, was only received in Washington on 15 September. Important events in Mexico were occurring without Washington's knowledge. Trist had finally made contact with Mexican peace commissioners on 27 August, but real progress only occurred after Scott's capture of Mexico City on 14 September and the fall of the Santa Anna government. A new government was organized in November which was willing to negotiate. However, authorities in Washington, unaware of the fall of the Mexican capitol and unhappy with what seemed to them long delays and no progress, sent a letter of recall to Trist on 6 October. The letter was only received by Trist on 16 November at a crucial stage in the negotiations.

Once the fall of Mexico City was known in Washington, many (including Buchanan) began to think that the instructions given to Trist were too liberal and that the whole of Mexico should be annexed. Trist, realizing that Washington was unaware of the true situation in Mexico, after considerable soul searching decided to ignore his recall and seized what he saw as a last opportunity to end the war by negotiating a treaty in accordance with his original instructions. Consequently, in a letter to his wife he asked her to inform Buchanan. The pertinent extract follows:[13]

Mexico, Dec. 4, '47

*....
P.S.

In my last (28th ulto) I desired you to say to Mr. B. that I have had a final irrevocable farewell to all official employment, and to give him my very best regards and most heartfelt regret at parting with him. Procure the key to this cypher (your sagacity will tell you where) and decipher the following to be read to him most secretly. This determination, I came to this day, at 12 o'clock. It is altogether my own.

Knowing it to be the very last chance, and impressed with the dreadful consequences to our country which cannot fail to attend the loss of that chance

15, 52, 39, 18, 65, 19, 1, 13, 3, 23, 58, 41, 10, 39, 29, 14, 27, 20, 61, 30, 7, 12, 45, 30, 9, 17, 29, 2, 3, 99, 23, 4, 41, 40 of 6, 114, 5, 73, 3, 215, 50, 27, 200, 44 and across 61, 115, 32°, 21, 41, 200, 41, 20, 24, 15, 75, 26, besides the 3, 121, 4, 36, 23, 26, 73.

Mrs. Trist's sagacity was up to the challenge. She deciphered the message as follows: "I will [make] a treaty if it can be done on the basis of up the Bravo and across by 32° giving 15 m[illion]s besides the 3 m[illion]s cash." This uses Weber's key in Figure 2. Trist intended to follow Polk's original orders by defining the boundary between the United States and Mexico as running from the Gulf of Mexico up the Rio Grande (known to the Mexicans as the Bravo) to 32 degrees north latitude and then west to the Pacific.

Trist was eventually successful and the resulting treaty took its name from the little village of Guadalupe Hidalgo where it was signed on 2 February 1848. Although Polk was unhappy, he could hardly disavow the draft instructions he had furnished Trist at the start of his mission. Against the advice of Buchanan, he sent the treaty to the Senate, which approved it on 10 March 1848 after much argument. Ratification by the Mexican Congress followed on 25 May 1848 and, as a result, the United States acquired California, New Mexico, Arizona, Nevada, Utah, and parts of Colorado and Wyoming. Edward Thornton wittily observed that Trist became the father of a healthy treaty nine months after his first interview with the Mexicans.[14] Trist had shown outstanding skill, tact, and patience in dealing with the chaotic diplomatic situation in Mexico and had achieved a surprisingly just settlement which has endured with relatively little friction to the present day.

Instead of the praise he merited, Trist was put under arrest, brought back to Washington in disgrace, removed from his State Department job, and not even paid for his expenses in Mexico after the date of his recall.[15] Trist found life very difficult after his return to Washington. Treated as an outcast, unable at first to find work, he eventually became a clerk on the Wilmington and Baltimore Railroad. His wife tried unsuccessfully to run a school for young ladies. Despite strong support from his friend Scott, who wrote in 1861 to Secretary of the Treasury Salmon P. Chase that Trist had been wronged by President Polk and neglected by Presidents Taylor, Fillmore, Pierce, and even Buchanan, nothing was done for him. In 1869 his always delicate health forced him to give up his railroad job. His cause was taken up by Senator Charles Sumner and the new administration of President Grant. In 1870 he was appointed postmaster at Alexandria, Virginia, and finally, in 1871 he was paid $14,559.90 for his salary and expenses in Mexico 23 years before, thus enabling him to spend his last few years in relative comfort. He died, several months after suffering a stroke, on 11 February 1874.[16]

The Search for Trist's Key Book

Only the first type of Trist's cipher can be read with the partial key reconstructed by Weber. To complete Weber's key and to decipher passages using Trist's second type of cipher it would be necessary to recover the key book which Trist used. Other investigators faced with similar problems have successfully identified such key books. For example, William F. Friedman recovered portions of a key text in the trial of Hindu conspirators in 1915. Later investigators found the book from which the key was drawn.[17]

Figure 3. Nicholas P. Trist from a Photograph Taken in his Old Age (Library of Congress)

VERDADEROS PRINCIPIOS

DE LA

LENGUA CASTELLANA;

OR,

True Principles of the Spanish Language:

CONTAINING

All the Rules necessary for acquiring a perfect knowledge of the Language; various Extracts and Translations in Prose and Poetry; Observations and Examples explanatory of the Analogies which exist between the Spanish Language and the Latin, French, and Italian:

TOGETHER WITH

AN APPENDIX,

CONTAINING

A TREATISE ON SPANISH SYNONIMS, AND A SELECTION OF PROVERBS IN SPANISH, FRENCH, AND ENGLISH.

Adapted for the Use of Schools, as well as of those who learn without a master.

By DON JOSE BORRAS,
Teacher of the Spanish and Italian Languages in the Belfast Academy.

BELFAST:

Printed by T. Mairs, Joy's-Court;
And Sold by Longman & Co., G. B. Whitaker, London: Oliver & Boyd, Edinburgh: John Cumming, Westley & Tyrrell, Dublin: and by M. Jellett, Belfast.

1827.

[PRICE FOUR SHILLINGS, IN BOARDS.]

Figure 4. Title Page From Trist's Key Book (Courtesy of the Louis-Lucien Bonaparte Collection, The Newberry Library, Chicago)

One of the present authors (Matyas) decided to try to find the book used by Trist as a key. He observed that in his letters of 3 June and 23 July 1847 to Buchanan, Trist described his key book--a small volume, with a prefatory address "To the British Nation," divided into at least two parts, and written by their old instructor in Washington, who was sent to Spain as consul. Weber's work had shown that the key text began with the words "The study of foreign languages...." With these slim clues Matyas set out to find the key book.

After some few preliminaries, including a search of the papers of James Buchanan that yielded no useful information about the key book, lists of all American diplomats in Spain and Spanish dependencies before 1847 were compiled from such sources as Congressional Directories and the 24 reels of microfilm containing correspondence from American consuls in Spain. The final list contained approximately 50 names. Consultation of the Library of Congress card catalog revealed that many of them were prolific authors. Their books included Washington Irving's Tales of the Alhambra and Legends of the Conquest of Spain, John Henry Eaton's Candid Appeal to the American, John Forsyth's Territorial Relations, Edward Church's Notice on the Beet Sugar, William Kirkpatrick's A Vocabulary, Persian, Arabic, and English, and even a small book entitled A Treatise on Milch Cows by Francis Guenon, translated for the Farmers' Library from the French, by none other than Nicholas Philip Trist himself. Examination of many of these books failed to uncover the key book.

Finally the name of Joseph Borras, consul at Barcelona from 1836, was suspected as being perhaps the Don Jose Borras who had published a small book entitled Verdaderos principios de la lengua castellana or, True Principles of the Spanish Language (Figure 4). The entry in the National Union Catalog indicated that this was a small book in English and that one of the few extant copies was located in the Newberry Library in Chicago. A member of their staff was kind enough to read the prefatory address from the book over the telephone to Matyas: "The study of foreign languages..." (Figure 5). His feelings were indescribable. Eureka! A year's tedious research had paid off. The key book had been found. But more important to Matyas, his painstakingly thorough research had proven fruitful.

The Verdaderos principios... was a very logical book for Trist to take on his Mexican mission. It was a small, handy compendium containing (as its title page stated) "all the Rules necessary for acquiring a perfect knowledge of the Language."

It was now possible to complete Weber's key for the first type of Trist's ciphers and also to decipher passages never before seen by historians that were written in his more secure second type of cipher. As Trist had written

in his letter of 23 July, Part Second, page 33, line 4, letter number 5 was the letter G.

An excerpt from Trist's dispatch No. 10 of 31 July 1847 (shown below) illustrates the use of both his first and second forms of cipher.[18] The first, based on numbering the letters in the key book's prefatory address, consists of a series of numbers separated by commas and dashes. (The dashes were used as fake word separators to confuse possible cryptanalysis.) The second form (or treble-numbered cipher), based on Part Second of the key book, consists of a series of numbers enclosed within slash marks: /...../. (Trist referred to them as brackets.) A series of three numbers within slash marks signifies the number of the page, the line, and the letter. When more than three numbers appear within the slash marks, all subsequent numbers signify letters in the same line. When two or more lines are used in succession from the same page, a double comma is written instead of repeating the page number:

Puebla, July 31/47

Hon: James Buchanan, Secretary of State

Sir,

In my last I said, "I consider the probabilities of an early peace very strong." The enclosed will be found to corroborate this belief. 1,2,3,10—15,13,4,1—39,26,11,31—44,75,121,31—/47,1,6,16/7,3,15,20,24,27,28,29/,,8,1,9/,,9,1/,,2,5/,,1,1/,,1,16,29/69,2,1/,, 6,7/,,2,3,2/,,6,4,6,10,8/ under date July 29: 5,33,25,4—30,105,44,45,58—from a foreign merchant to this correspondent here....

If the letters of the prefatory address of Trist's key book (Figure 5) are numbered consecutively to develop a key (Figure 6) and the key is then used to decipher the above numbers up to the first slash mark (written in the first, of simple, form of Trist's cipher), the text is recovered as:

t h e	f i r s t	i s	f r o m	m r
1,2,3,	10—15,13,4,1—	39,26,	11,31—44,75,	121,31—

The ciphertext using the second (or more complex cipher) is replete with errors and more difficult to decipher. Three mistakes must be corrected in the excerpt above for a proper decipherment. The number 46 must be inserted between the second and third slash marks: /46,7,3,15,20,24,27,28,29/. (Trist had changed pages in the key book without making the proper indication.) Similarly, the number 47 must replace the double commas between the seventh and eighth slash marks: /47,1,16,29/ (Trist does it again!), and the number 1

must be inserted between the ninth and tenth slash marks: /,,1,6,7/. (Trist has forgotten the line number.)

TO THE BRITISH NATION.

THE study of foreign languages, after the acquisition of our own, is undoubtedly one of the most interesting and agreeable, which can occupy the time of literary persons, or engage the attention of those who are desirous of presenting themselves in society, as objects of a polite and accomplished education.

The Spanish Language, which yields to none in elegance, expression, or strength, has now become, by reason of commercial treaties recently established with South America, as necessary and important to the British youth, as it is instructive and entertaining to the learned, by reason of the infinite number of works, which in all times, and on all subjects, have been written (notwithstanding the trammels of the Inquisition) by men of genius, in that once eminent, but now unfortunate country.

The study of this language, which for almost a century was but little attended to in this country, has now began to be revived, and it is the duty of those who profess to teach it, to render its acquisition as easy, and as interesting as the dryness of grammatical rules will permit.

It is not my intention to censure the methods pursued by different authors in communicating a knowledge of the Spanish Language; but as it is my own opinion that languages are more easily learned by *practice* than by *Grammar*, and that the latter is only useful in proportion as its rules are expressed with simplicity and brevity, I have composed this Work, to which I have given the title—"VERDADEROS PRINCIPIOS DE LA LENGUA CASTELLANA."

In composing the following Work, I have departed from the system too generally followed, of multiplying rules and examples, for the most part contradictory and obscure, and which serve rather

* See A. Anaya's English Treatise on Spanish Literature; also another on the same subject, in Italian, by Saverio Lampillas

Figure 5. Prefatory Address from Trist's Key Book (Courtesy of the Louis-Lucien Bonaparte Collection, The Newberry Library, Chicago)

thestudyof	(10)	esinsociet	(210)	saryandimp	(410)
foreignlan	(20)	yasobjects	(220)	ortanttoth	(420)
guagesafte	(30)	ofapolitea	(230)	ebritishyo	(430)
rtheacquis	(40)	ndaccompli	(240)	uthasitisi	(440)
itionofour	(50)	shededucat	(250)	nstructive	(450)
ownisundou	(60)	ionthespan	(260)	andenterta	(460)
btedlyoneo	(70)	ishlanguag	(270)	iningtothe	(470)
fthemostin	(80)	ewhichyiel	(280)	learnedbyr	(480)
terestinga	(90)	dstononein	(290)	easonofthe	(490)
ndagreeabl	(100)	eleganceex	(300)	infinitenu	(500)
ewhichcano	(110)	pressionor	(310)	mberofwork	(510)
ccupytheti	(120)	strengthha	(320)	swhichinal	(520)
meoflitera	(130)	snowbecome	(330)	1timesando	(530)
rypersonso	(140)	byreasonof	(340)	nallsubjec	(540)
rengagethe	(150)	commercial	(350)		
attentiono	(160)	treatiesre	(360)		
fthosewhoa	(170)	centlyesta	(370)		
redesirous	(180)	blishedwit	(380)		
ofpresenti	(190)	hsouthamer	(390)		
ngthemselv	(200)	icaasnecs	(400)		

Figure 6. Trist's cipher Key Obtained from Prefatory Address in Key Book.

The lines of text from Part Second of the key book necessary to decipher the text corresponding to the second type of cipher are listed below in the order of their use by Trist:

Page, Line	Text
	6 16
47,1	FABLE TWENTY-FIFTH — The Fly and the Bull.
	3 15 20 24 27 28 29
46,7	me habla? pregunto el toro, con un t o n o brutal.
	1 9
46,8	Soy yo. Quien? Aqui estoy. Oh, senora mos-
	1
46,9	ca! es vm. quien me habla? vm. no es tan pesada
	5
46,2	UNA mosca se puso sobre el cuerno do un toro, y
	1
46,1	FABULA VEGESIMA QUINTA.—La Mosca y el Toro.
	16 29
47,1	FABLE TWENTY-FIFTH — The Fly and the Bull

```
                1
69,2    magnificencia a los mas celebres del Imperio:  y
                     67
69,1    consules no inferiories en valor, en prudencia, y en
                 23
69,2    magnificencia a los mas celebres del Imperio:  y
                    4 6 8 10
69,6    del triunfo fueron tambien Espanoles; y finalmente
```

(Complete pages 46, 47, and 69 from Part Second of the key book are reproduced in Figures 7, 8, and 9, respectively.) The corrected ciphertext and the decipherment of the second type of Trist cipher is:

```
      t h     h o r n t o n     s e     c     o
/47,1,6,16/46,7,3,15,20,24,27,28,29/,,8,1,9/,,9,1/,,2,5/

      f       h b       m     l e     g a     t i o n
,,1,1/47,1,16,29/69,2,1/,,1,6,7/,,2,3,2/,,6,4,6,10,8/.
```

The remainder of the cipher text is in the first form of Trist's cipher and presents no difficulties:

```
t h e   s   e c   o n d
5,33,25,  4—30,105,44,45,58
```

So the complete decipherment of the 31 July 1847 excerpt reads thus: "the first is from Mr. Thornton sec[retary] of H[er] B[ritannic] M[ajesty's] legation under date July 29: the second from a foreign merchant to this correspondent here...."

One can only imagine the frustration and exasperation of the State Department cipher clerks trying to decipher Trist's dispatches and having constantly to make adjustments to correct his errors. Despite his clumsy, error-prone ciphers, Trist should be given considerable credit for his patience, perseverance, and diplomatic skill in bringing the Treaty of Guadalupe Hidalgo to a successful conclusion.

ACKNOWLEDGEMENTS

The authors wish to thank Professor Ralph E. Weber for initially acquainting them with Trist's ciphers. An earlier form of this article was presented at the Third Beale Cipher Symposium, Crystal City, Virginia, on 12 September 1981.

FABULA VIGESIMA QUINTA.—*La Mosca y el Toro.*

UNA mosca se puso sobre el cuerno de un toro, y temiendo incomodarle con su peso, le dixo: perdone vm. señor la libertad que me he tomado; pero si cree que pese demasiado sobre vuestra cabeza, volaré; vm, puede mandarme con franqueza. ¿Quien me habla? preguntó el toro, con un tono brutal. Soy yo. ¿Quien? Aquí estoy. ¡Oh, señora mosca! ¿es vm. quien me habla? vm. no es tan pesada como se imagina, y en verdad que no advertí quando se puso vm, sobre mi cabeza, ni creo que me aperciba quando vm, quiera cambiar de lugar.—Es demasiado comun encontrar personas que creen ser de conseqüencia, no siendo su espiritu mas grande que el de la Mosca: mas estos tontos llenos de vanidad vienen á ser la risa de los que conocen su merito y calidad.

FABULA VIGESIMA SEXTA.—*El Gallo y la Hormiga.*

UN gallo *se paseaba* con sus pollos en un bosque, y recogian *de paso* los *granos* que encontraban. Viendo el gallo un *hormiguero* reunió *á* sus hijos para decirles, ved ahí un tesoro: no temais, y comed sin ceremonia estos insectos; una hormiga es un bocado goloso para un polluelo: ¡que felices seriamos si pudiesemos escapar del cuchillo del cocinero! En verdad *el* hombre es bien cruel é injusto en destruirnos para satisfacer su golosina. Una hormiga que trepó á un arbol oyendo lo que discurria el gallo, le dixo: Antes de tildar los defectos de otros exâmine vm. su propia conciencia: vm, no deberia por un solo almuerzo destruir un hormiguero.—Vemos las faltas de los otros y estamos ciegos para mirar las nuestras.

FABULA VIGESIMA SEPTIMA.—*Las dos Zorras.*

Una noche entráron dos zorras furtivamente en un gallinero: matáron el gallo, las gallinas, y los

Figure 7. Page 46, Part Second, from Trist's Key Book (Courtesy of the Louis-Lucien Bonaparte Collection, The Newberry Library, Chicago)

FABLE TWENTY-FIFTH.—*The Fly and the Bull.*

A FLY having seated himself on a bull's horn, and being afraid of incommoding him by his weight, said to him: pardon, sir, the liberty I have taken; but if you feel any inconvenience from my weight on your head, I shall fly away; you may freely command me. Who speaks? enquired the bull in a brutal tone. 'Tis I. Who? Here I am. Oh, madam fly! Is it you who were speaking to me? you are not so heavy as you imagine; indeed I did not feel you when you alighted on my head, nor do I think that I shall be sensible of the change when you fly off.—We too frequently meet with persons who think themselves of consequence, but whose spirit is as contracted as that of the fly: such vain fools, however, become the laughter of those who know their real merit.

FABLE TWENTY-SIXTH.—*The Cock and the Ant.*

A COCK *was taking a walk* in a wood with his chickens, who were gathering the *grains of corn* which they found *in passing.* The cock seeing an *ant's nest* collected his chickens and said: Behold a treasure; eat those little insects, and be not afraid; an ant is a dainty morsel for a young chicken: how happy should we be if we were only able to escape the cook's knife. Man is really very cruel and unjust to destroy us, for the purpose of satisfying his gluttony. An ant that was climbing a tree, hearing what the cock was discoursing of, said to him: Before censuring the errors of others, examine well your own conscience: you ought not for one single breakfast, to destroy a whole nest of ants.—We see the faults of others, but are blind to our own.

FABLE TWENTY-SEVENTH.—*The Two Foxes.*

ONE night two foxes entered by stealth into a hen-roost; they killed the cock, the hens, and the

Figure 8. Page 47, Part Second, from Trist's Key Book (Courtesy of the Louis-Lucien Bonaparte Collection, The Newberry Library, Chicago)

consules no inferiores en valor, en prudencia, y en magnificencia á los mas celebres del Imperio: y consules que hermosearon á Roma con monumentos iguales á los de Pompeo y de Augusto. Los primeros extrangeros que en Roma obtubieron el honor del triunfo fueron tambien Españoles; y finalmente lo fueron *Trajano, Adriano, Alonso,* y el *Gran Teodosio* que empuñaron el cetro Imperial de Roma, sobrepujando con sus acciones y virtudes la gloria de los Cesares.

Tales fueron los Españoles en tiempo de la soberbia Roma: exâminemos lo que fueron despues, lo que son aora, y las causas de esta monstruosa decadencia.

Si la España Pagana se distinguió por su sabiduria y valor no admiró menos á la Europa la España Christiana. En el primer siglo de la Iglesia Romana los Españoles se dedicaron con especial zelo á ilustrar y promover los estudios sagrados con sapientisimas obras que diéron á luz los grandes hombres de aquel siglo. La sede Romana se vió ilustrada por muchos años por Pontifices Españoles benemeritos no menos á la religion que á la sagrada literatura; y en quanto lo permitieron las guerras y dominaciones que sufrió nunca dejaron los Españoles de acreditar su *sabiduria* y *valor.* Entre las muchas obras que escrivió en el Siglo XIII. Alonso el sabio Emperador y Rey de Castilla y Leon, ya como matematico y astronomo, ya como historiador y poeta, se cuenta una *Parafrasis* de la *Historia Biblica* y *Sagrada.* En el mismo Siglo, el Gran Santo Domingo promovió en la Unviersidad de Boloña el Estudio de la *Sagrada Escritura,* y lo mismo hicieron despues el prodigioso Peñafort y el Cardenal Albornóz. Pero quando la moral y la luz que resplandece en la *Santa Biblia* iluminaba á los hombres, se introduxo el error y abuso mas lamentable que fue *el de dar el poder del* MUNDO, *á los que han, renunciado el* MUNDO: Los primeros Papas no se mezclaban en los asuntos temporales ó Civiles, sino para

Figure 9. Page 69, Part Second, from Trist's Key Book (Courtesy of the Louis-Lucien Bonaparte Collection, The Newberry Library, Chicago)

REFERENCES

1. Richard M. Ketchum, "The Thankless Task of Nicholas Trist," American Heritage, 21 (August 1970), 13.
2. Ibid., 14.
3. Louis M. Sears, "Nicholas P. Trist, a Diplomat with Ideals," Mississippi Valley Historical Review, 11(June 1924), 88-89.
4. Ibid., 93.
5. General Records of the Department of State, Record Group 59, Despatches from United States Ministers to Mexico, 1823-1906, Microcopy 97, 197 rolls; National Archives, Washington, D.C., Microfilm Roll 15 (hereafter cited as General Records of the Department of State RG 59, M 97, Roll 15).
6. Ralph E. Weber, United States Diplomatic Codes and Ciphers (Chicago, 1979), 23-24.
7. James B. Ward, The Beale Papers, (Lynchburg, 1885), 20-22. Reprinted by The Beale Cypher Association, P.O. Box 216, Medfield, MA 02052.
8. Carl Van Doren, Secret History of the American Revolution (New York, 1969), 200.
9. Albert C. Leighton, "Secret Ciphers in Bavarian Archives," Proceedings of the Second Beale Cipher Symposium (1979), p.79.
10. Examples are: Ketchum; Sears; Robert Arthur Brent, Nicholas Philip Trist: Biography of a Disobedient Diplomat (Ph.D. dissertation, University of Virginia, 1950); Eugene Keith Chamberlain, "Nicholas Trist and Baja California," Pacific Historical Review, 32,(1963), 49-63; Kenneth M. Johnson, "Baja California and the Treaty of Guadalupe Hidalgo," Journal of the West, 11 (April 1972), 328-347; Don Blevins, "The Forgotten Peacemaker, Nicholas Trist," American History Illustrated, 14 (June 1979), 4-8, 42-47.
11. Weber, 205-206.
12. General Records of the Department of State RG 59, M 97, Roll 15.
13. Papers of Nicholas Trist, Vol. 25, Library of Congress, Washington, D.C.
14. Sears, 96.
15. Ketchum, 89.
16. Ketchum, 89.
17. David Kahn, The Codebreakers (New York, 1967), 372-373.
18. General Records of the Department of State RG 59, M 97, Roll 15.

FROM THE ARCHIVES

EXAMPLES OF INTELLIGENCE OBTAINED FROM CRYPTANALYSIS

1 AUGUST 1946

(Declassified per Sec. 3, E. O. 12385 by
Director, NSA/Chief, CSS, 6 October 1980.)

[Ed. Note. During the course of their research, our editors and readers are sometimes responsible for the declassification of previously undisclosed material. Or they may discover items in private or public collections, libraries, and archives, items which are not widely known. The purpose of this column is to give these documents wider circulation for the benefit of the cryptologic community. If you have or know about material suitable for this column, please send it to David Kahn, 120 Wooleys Lane, Great Neck, NY 11566. All contributions used will credit the donor.]

[Louis Kruh ran across a reference to this column's document and requested a declassification review. As a result, it was declassified on 6 October 1980. Some sections are sanitized, i.e. deleted, because the authorities feel they are not releasable under current classification regulations. The text contains the gaps caused by the excisions, except where such gaps are excessive and their true length of the gap is indicated.]

[The following item, dated 1 August 1946, is now in the National Archives, Record Group 457, Item SRH-066. — Ed.]

INTRODUCTION

The following examples are selected from the files of the Army Security Agency to illustrate the different kinds of information obtained from cryptanalysis of enemy messages and, where possible, the action taken and results achieved. Two of the examples also indicate the importance of protecting this source of information.

I. Japanese Army Systems

A. The Hi-81 and Mi-27 Convoys November 1944

1. On 14 November 1944 the First Transport Staff in Moji sent a cryptograph radio message to the airforce units concerned requesting air escort for two convoys, the Hi-81 and Mi-27, carrying troops to reinforce the Philippines. According to the message, which was read by the Army Security Agency, one of the convoys consisted of ten ships, tankers and escort vessels; it was to leave Mutsure on the 15th; the route, including noon positions from the 15th through the 22nd, was given. (J11925) The convoys immediately encountered difficulties. According to a series of Japanese Navy messages which were read by the United States Navy, the Akitsu Maru was sunk by a submarine on 15 November. On 17 November the Hi-81 reported being sighted by a B-29, with strong indications that the Mi-27 had also been sighted. Four hours later the Mayasan Maru was torpedoed. The final score for both convoys according to messages read by the Army Security Agency, was six ships definitely sunk, one ship disabled and one ship on fire. (J3273, J3259, J44932, J16120, J16852) The diaries of two of the survivors, which were later picked up in the Philippines, confirmed the information obtained from the messages on the serious damage inflicted on the convoy and added that one aircraft carrier was also sunk.

2. This episode may be used to illustrate another important aspect of the work of obtaining intelligence from enemy traffic. The careful study of the external aspects of messages by the sections dealing with traffic analysis made it possible to recognize a convoy message in raw traffic, and to concentrate all efforts on translating it in time to be of use.

3. Another point illustrated by the history of the Hi-81 and Mi-27 convoys is the method adopted to protect the source of information. The sighting of the convoys by B-29's explained to the enemy the submarine attack.

B. The Japanese Attack on Aitape, 10 July 1944

1. A summary of the Aitape-Wewak operations in the summer of 1944 illustrates how useful this type of information may be in making estimates for the planning of operations. Messages read early in the year at Central Bureau, Australia showed the status of Japanese forces in the area between Madang and Hollandia; the existence of acute supply problems was revealed and the number of front line troops together with the state of arms and equipment was given. The subsequent withdrawal of these units into the Wewak area was not unexpected to the American command. By the end of May the Japanese found their position untenable and decided to attack. A 28 May message, which was translated by the Army Security Agency on 1 June, mentioned supplies needed by the 18th Army, controlling operations in eastern New Guinea, which must arrive at Wewak by the end of June in order to be of use in "the attack of Aitape." (F13408) A 20 June message from the 18th Army translated 25 June, supplied the information that an all-out attack against the US Aitape perimeter was to begin about 10 July. The message gave the detailed disposition of each division under the command of the Army with the planned operations of each division in attack; total strength of the forces involved was stated to be about 20,000. (F19959)

2. The information was forwarded to the Commander in Chief, Southwest Pacific Area. The Japanese attack was made on schedule, and the results were reported in a message of 13 August: According to the report of the Japanese Commander, most of the enemy artillery had been destroyed, the units decimated. The seriousness of the supply situation was shown by the description of how they had made their ten days' supply of rice last twenty-five days; "By resorting to chewing it raw instead of cooking it, the period of consumption had been prolonged somewhat." The Commander concluded that, "Unless we can impress upon the enemy the greatness of the defensive strength of the Japanese Army, thereby striking terror into his heart, it will be impossible to defeat the enemy." (F25591)

C. The Tachibana Maru, summer of 1945

1. Early in 1945 it became apparent from reading Japanese traffic, that the enemy was attempting to redeploy their forces in the Netherlands East Indies. One of their objects was to withdraw units from the Banda

Sea area to the comparative safety of Java and Sumatra. By June however lack of available water transport lad them to try to make use of a hospital ship, the Tachibana Maru, for purposes other than those prescribed by the Geneva Convention. (J74568) The ship was renamed the Hirose Maru (J71916) and assigned to transport 1500 troops of the 11th Infantry Regiment with 150 tons of ordnance and munitions from Tual in the Kri Islands to Surabaya. (J77567) Precautions taken to provide against the possibility of search by an enemy vessel included supplying hospital clothing for the troops, having available daily sick reports and lists of medical supplies (J77567) and sending the regimental colors by air. (J89766) The ship left Tual 1 August, scheduled to reach Surabaya on the 5th. (J91835)

2. According to the New York Times' account however, the Tachibana, although marked by floodlighted red crosses twenty feet high, was halted north of Timor by two destroyers. The discovery by a search party that cases marked medical supplies contained munitions, while the only wound among the hospital patients was the result of a packing case being dropped on a thumb, led to the capture of the ship. (New York Times, 5 Aug 45; 8 Aug 45)

3. Fully one month before this attempted deception, information about the Japanese plans for the unorthodox use of the hospital ship had been received from messages. Other messages translated in July made it possible to give the Navy exact information on ports of arrival and departure and loading and sailing times. Again the source was concealed by attributing the sighting of the ship to air reconnaissance. (New York Times, 8 Aug 45)

II. Japanese Military Attaché Systems

A. Japanese Description of the West Wall, November 1943

1. The value of intercepted diplomatic and military attaché traffic for military intelligence purposes is illustrated by quotations from the report of Colonel Ito, attached to the German Western Area Headquarters, who made the report after inspecting the Atlantic coast defenses in the autumn of 1943.

In the construction and location of fortifications, emphasis is mainly on the defense against landings at and the protection of the naval bases, especially the five submarine bases of Brest, L'Orient, St. Nazaite, La Rochelle and Bordeaux...The harbors, large and small, have been fortified with emphasis on the proper weapons and defenses for each particular location. We have confirmed the fact that defenses of places

other than those with cliffs and precipices have all been fortified for more than 1,000 meters from the shore line. In the places where there are cliffs and precipices, a sharp lookout is kept. They have arranged things so that troops are held in reserve in the rear and can be immediately sent in as reinforcements...In order to protect her submarine bases and harbors, Germany has not only constructed defenses against sea attack, but has made powerful land from defenses...consists in constructing for several kilometers from the harbors defensive positions which connect nests of resistance and strong points. This defense varies in depth for the various cities as follows

La Rochelle...10 to 15 kilometers
Le Harre...6 to 8 kilometers
Cherbourg...7 kilometers
Boulogne 4 to 5 kilometers
Dieppe 2 to 3 kilometers

Examples of the types of army and navy coastal type guns used on the sea front in the defense of harbors:

La Rochelle district - four 60 caliber 200 mm. naval guns; four 35 caliber —m— —m— —m— mm. army guns.
Royan district - four 280 mm. naval guns
Le Havre district - four 300 mm. guns
SHIEABURAWA (kana version of place name. May be Cherbourg) district - four 380 mm. heavy field pieces...

In order to eliminate dead space in the neighborhood of the strong points, they have two or three grenade throwers firing from within the armored turret (?range?) 20 to 600 meters; speed of fire - 120 per minute; caliber, 50 mm. --g-- --g—. These are high-angle fire weapons. For defense against tanks, tank ditches (built in triangular cross-section with a span across the top of 5 meters and a depth of 3.5 meters) are constructed along the periphery of the strong points. In addition to having flanking fire provided by 2 or 3 casemates with 40 mm. Skoda anti-tank guns (?similar to?) machine guns and 2 or 3 casemates with 60 caliber 50 mm. anti-tank guns, they have 2 or 3 gun shelters (Protected against bullets) with 60 caliber 50 mm. anti-tank guns which they can drag out into the open to fight when the opportune moment comes. They also have mine fields in front of and behind the tank ditches (anti-tank mines, anti-personnel and horse mines, etc., are used together; they are laid in three rows of 2 mines each for each 3 square meters). As for as infantry obstacles are concerned, in addition to the mine fields, they have wire entanglements both in back of the

tank ditches and within the strong points. For the direct protection of the casemates, fixed-type flame throwers are buried in the ground nearby and set up so that they can be electrically ignited from the ringstelle. (D3348)

B. The OSS in Lisbon

1. General Marshall in his letter to Governor Dewey of 25 September 1944, gave as an example of "the delicacy of the situation" that "some of Donovan's people (OSS), without telling us, instituted a secret search of the Japanese Embassy offices in Portugal. As a result the entire military attaché Japanese code all over the world was changed, and though this occurred over a year ago, we have not yet been able to break the new code and have thus lost this invaluable source of information, particularly regarding the European situation." (New York Times, 8 December 1945)

2. A series of Japanese messages, read by the Army Security Agency, gives a behind the scenes picture of the repercussions of this episode. The OSS although misguided, apparently carried on their operations with some skill, since the first news that "American espionage agency in Lisbon knews minutest details of activities of Japanese ministry there and also has the Japanese codebook" came from the Italian General Staff in Rome (Rome/Tokyo, 6/29/43, ; Rome Circ. 6/29/43, D1318)and was a complete surprise to Morishima, the Japanese minister in Lisbon. He assured Tokyo that "code books ...could hardly have been stolen, because of careful precautions...Perhaps," he suggested, "you mean some of the messages were deciphered." He naturally wished to know the source of the Italian information. (Lisbon/Tokyo, 6/30/43, This point was never settled, according to the correspondence, but it was suggested that the report might have come from "...an Italian resident in Lisbon who has contacts with British and US Intelligence Agencies." The Japanese Legation continued to assert that it was impossible that "...their materials could have been seen by any unauthorized person." (Lisbon/Tokyo 7/2/43, D-1316) An investigator, however, was sent to Lisbon where he was "resented and ill-treated." (Madrid/Tokyo, 7/12/43)

Morishima then offered his resignation (Lisbon/Tokyo, 8/25/43, and his fellow-minister in Madrid thought it "only natural that he should be indignant and utterly discouraged" at this high-handed treatment. (Madrid/Tokyo, 8/26/43)

3. Although this ill-advised attempt to procure a copy of a codebook which was already being read apparently had results, they were not as disastrous as General Marshall's letter indicated. The code was not

changed but on 18 September 1943, the Japanese introduced a new and more complicated system of enciphering the code. By the beginning of December of the same year, however, the new key had been solved and messages in the Japanese military attaché system were again being read by the Army Security Agency.

III. German Diplomatic System

A. Oscar Hellmuth, Secret Agent, 1943

1. The Blue Book on Argentina, the United States Government official indictment of the fascist regime in that country, emphasizes strongly the importance to the cause of the Allies of the arrest of Oscar Hellmuth. In 1943 the Argentine Government was negotiating with the Nazis in order to obtain German arms which were to be used to strengthen Argentina in her position of refusing to break relations with the Axis. According to the Blue Book the negotiations "culminated in October 1943 in the ill-starred Hellmuth mission...The Argentine Government and Himmler's secret intelligence agents in Argentina selected Oscar Hellmuth, an Argentine national, as their common representative to enter into broad negotiations with the German Government in Berlin, not only for arms, but for many other types of mutual assistance. The mission failed but only because of Hellmuth's arrest en route by the Allies." He was removed from the ship on which he was travelling to Spain by British authorities in Trinidad in October 1943. (New York Times, 26 Jan 1944)

2. It is possible that the information which led to Hellmuth's arrest came from a message read by the Army Security Agency, which was sent by the German Chargé d'Affaires in Buenos Aires to Berlin, 30 September 1943, in which he reported the intention of the Argentine Government to send Hellmuth, described as a co-worker of the Germans in Buenos Aires, via Spain to Berlin where he was to be received by the Fuehrer. This message was translated 24 October, six days before the arrest of Hellmuth in Trinidad. Coast Guard messages supplied the name of the ship on which he sailed.

B. Cargo of Monte Albertia

1. According to the New York Times, the Minister of Economic Warfare announced in London in November 1943 that some weeks before "five ships plying between Buenos Aires and Spain were halted and British control points for search with the following melodramatic results: 40 drums stated on navicerts as containing paste were found full of liver

extract, an important base in food compound for U-boat crews. Twelve drums had false bottoms and embedded in each was a disk of platinum three inches in diameter and weighing a pound, worth more than $4,000 apiece but worth a king's ransom to Germany as a factor in the manufacturing of nitroglycerine for explosives. Also in the cargo were six tons certified as bacteriological peptone when in fact they were stuffed with small containers of gland extract powder for the treatment of shock. In making public this discovery the British showed what they and the Americans, with whom they are in close touch, are up against, as well as how the system is working. (New York Times, 10 Nov 1943)

2. A series of messages between Erich Otto Meynen, the German Chargé d'Affaires in Buenos Aires, and Berlin, which were read by the Army Security Agency, revealed very clearly how the smuggling system worked. Ships officers or Argentine nationals were found who were willing to act as agents; their chief function, apparently, was to deliver the consignments to the German consul in the first harbor which the ships touched. In a message of 16 August 1943 translated 30 August, the arrangements for the cargo sent on the Monte Albertia, a Spanish cargo ship, were described: 40 boxes which had been declared as containing bile paste really consisted of "extract"; twelve of them had false bottoms covering 56 kilograms of platinum. Six boxes which supposedly consisted of peptone in reality contained pituitary extract.

IV. German Low Echelon Army Systems

A. Signal Intelligence Operations in the Field

1. The Operational History of the 349th Signal Intelligence Service, Mediterranean Theater of Operations, describes the nature of the intelligence produced by radio intelligence organizations, which attacked enemy low and medium security traffic in the field. In comparatively static periods, attended by low volumes of radio traffic, information obtained from these types of enemy messages tended to deal with such topics as strength reports and ammunition returns, artillery and mortar fire orders, relief of personnel and changes of position, patrol activity and location of enemy units and positions. Intelligence of this kind made it possible to maintain a constant check on enemy activities, intentions and dispositions; to keep order of battle files up to date; and to know in advance or proposed Allied targets and possible enemy target points, on the basis of which the latter were often shelled or bombed successfully. During times of tactical activity, when radio activity also, of course, increased, enemy traffic

supplied up-to-the-minute, play by play descriptions of engagements, often before the information was received from Allied troops, and betrayed enemy intentions and relocations before their actual execution.

2. Some illustrations of this type of intelligence and the use to which it was put are taken from the account of the operations of Detachment E, 849th SIS, in Italy: "As the Allied forces crossed the Volturno the mobile 3 Panzer Grenadier Division was identified on 12 October as coming into the line, suggesting that it was to cover further withdrawal and that the enemy did not intend to make a stand at the river line. Three days later the line was revealed to run generally from Ameglio to Ailan to S. Massima." (p. 42) "When the enemy inland forces were withdrawing along the main route across the Mignano bridge, Allied bombers attacked the bridge the morning of 20 October, but could not determine the damage. By noon the Hermann Goering Engineers code was broken and revealed that the bridge had been destroyed beyond immediate repair and that traffic was to be re-routed through Conca. Early that afternoon the enemy alternate route of withdrawal was put under attack and bottled up." (p. 43) At Anzio: "Early realizing the important part artillery was to play in the enemy attempt to contain the beachhead, changes in the operating set-up were effected which brought the application of Signal Intelligence to a peak of effectiveness. Single isolated messages would not suffice. Detailed records were kept of each individual enemy group, of every location, mission and the number of rounds fired. Four of the Intelligence Staff men were assigned to keep a constant watch on voice frequencies. Although the enemy re-enciphered the code some five times, continuity in reading the code was maintained throughout the operation. So detailed was the tabulation kept of radio reports that at any given time it was known just how many rounds a given battery had expended or how much ammunition it had received, or what its alternate position was. So close was the liaison with Allied counterbattery that enemy reports of Allied fire were used as correction data for Allied firing guns." (p.44) "On 24 May with the main VI Corps attack northward toward Cori, messages on the 105 Flak Regiment net showed that some 4 or 5 of its Battalions were located between the 335-365 northings and 912-961 eastings. Since this unit had been operating in a ground anti-tank role, it clearly showed that the enemy expected an armored thrust to the Northwest, which indeed was the plan. At about this time the decision was made to move troops over the mountain, which soon hopelessly split the enemy forces." (p.45)

3. Similar examples may be found in the Third Army Radio Intelligence History in Campaign of Western Europe, prepared by Signal Intelligence Service of Headquarters Third U.S. Army. For instance, "As early as D-

day itself, reconnaissance traffic of the 21 Panzer Division was intercepted on the English side of the Channel indicating the formation's commitment in the Caen sector." (p.31) "Headline news on 31 July came with the disclosure that 2 SS Panzer division headquarters was located at Montbray, and, on the same day the need of ammunition by the Division's artillery regiment was expressed in traffic formation." (p.32) "Reconnaissance patrals of 21 Panzer Division on the 16th of August provided the highlight of activity to that date giving extensive reports on the situation at the south end of the Falaise Gap. 2 Panzer Division was mentioned as 'the left flank neighbor'; and tanks of the 9 SS Panzer Division were reported in Lacourbe and Montgaroult. The reconnaissance missions of this group shifted the following day to an area east of Falaise and continued their conveniently detailed reports indicating that it was one of the principal units covering the withdrawal east from the gap to the Seine." (p.34) "The high point of the month's spot intelligence came on the evening of 28 September at 1815 hours when a reconnaissance patrol announced that Battalion 'Schneider' would attack on the following morning at 0600 in the vicinity of Foret de Gremmercy to establish contact with its left neighbor. As the reconnaissance traffic reported the next day, this attack was repulsed." (p.40)

4. The mission assigned to Signal Security Detachment "D" was the procurement of signal intelligence from the solution of tactical codes and ciphers for the Acting Chief of Staff, G-2, 12th Army Group. (Summary of Operational Activity, Signal Security Detachment "D" for the Period 1 September 1944 to 1 April 1945.) "During the German Ardennes offensive, messages from thirteen divisional and similar formations in and near the 'Bulge' was read. Since the formations represented the bulk of the armored and mobile formations employed by the Germans during the Ardenne operations and constituted the major threat to Allied forces, the intelligence gained from their messages not only indicated accurately the trend of enemy operations carried out by all enemy units within the 'Bulge' but also provided G-2 with reliable information at a time when other intelligence sources were relatively unproductive or non-existent." (An Analysis of Ciro-Pearl Intelligence derived from German Army Signal Communications by Signal Security Detachment "D" during the Period 10 August 1944 - 12 May 1945. p.2) "In early September 1944, when the German Armies were rapidly retreating through eastern France and Belgium to the Siegfried Line, 2 SS PZ Div 'Das Reich' was retiring southeastward from the line: Dinant-Liege, Belgium. On 7 September 1944, the Div Ia (operations) of 2 SS PZ DIV announced to Div elements that: 'The Allies have presumably reached Liege from the West. 12 SS PZ Div "Hitler Jugend" now has its furtherest forward Outguard Line of Resistance west of Hamoir." The usefullness of this

information at a time when Allied elements were feeling out an otherwise confused situation in the Liege area was immediate."(ibid, pp. 4-5) "During the rapid retreat of the German armies in France and Belgium in September 1944, 9 PZ Div...communications of 28 September announced the location of a large fuel and ammo dump...in the forest 3 km from Villers -Cotterets. (Note - the above mentioned dump was the largest supply dump captured intact in France. Two German general officers were surprised at breakfast when Allied armored forces took the area under command.)" (ibid, p.7)

THE ADVENT OF CRYPTOLOGY IN THE GAME OF BRIDGE

PETER WINKLER

ABSTRACT: The surprising discovery that information can be passed both covertly and legally between bridge partners has added a new dimension to the theory of this popular game. In this paper some of the methods are sketched and their cryptologic foundation is described.

KEYWORDS: Cryptology, bridge.

The recent introduction of cryptologic techniques into bidding and defense in bridge has generated interest and controversy on both sides of the Atlantic, and threatens to add a significant new dimension to the theory of the game. We believe this development to be of interest to the cryptologic community, partly because there are some interesting aspects concerning the creation of key from partial information, but also because there is a possibility that some fraction of the large number of serious bridge players may, as a result, become interested in cryptology.

Of the three major activities--bidding, defense and dummy play--that comprise the game of bridge, the first two require cooperation between partners. It is thus desirable in both cases to communicate as much information as possible to one's partner, while giving as little as possible to the opponents. This procedure is made difficult to achieve by two laws of the game: (1) all communication must be done via legal calls and card plays; and (2) partnerships may not have private agreements (e.g., about the meaning of some call or play.)

It is thus not surprising that, until recently, secret communication with one's partner was generally regarded as solely the province of cheaters. Ethical bridge players concentrated on communicating whatever information seemed to be more likely to help partner than the opponents. In doing this they are permitted to have prior agreements--possibly of very complex and artificial nature--between partners, but all such agreements must be revealed in advance to the opponents.

Suppose, for example, that in the course of bidding toward a slam South wishes to tell his partner (North) that he holds the ace of clubs. He can usually do this by making some appropriate call (e.g. a cue-bid of Four Clubs) but the opponents may also benefit from this information, particularly in the selection of opening lead. For South instead to write a note and pass it under the table to North would obviously be a violation of law (1). Alternatively, the North-South partnership might have an understanding that in the present auction a bid of Four Hearts shows the ace of clubs; but then law (2) requires that the agreement be made known in advance to the opponents.

Nonetheless, the information that South has the ace of clubs is sometimes passed to North in covert but legal fashion. If North, holding the other three aces, were to employ some ace-asking convention (such as Blackwood) and receive a one-ace reply, he would know of course that his partner's ace is in clubs; but no law requires North to reveal to the opponents what he can deduce from looking at his own hand. This instance is of little practical importance, since when North-South hold all the aces the opponents are not likely to care who holds which.

On the other hand, once one piece of information has been passed covertly it can be used as key for another: thus, conceivably, South's next bid might carry the message "I hold the king of the suit in which I hold the ace."

The following example is intended to reduce the situation to its simplest cryptographic terms. Suppose each of three people, A, B and C, is dealt a random card from a deck consisting only of the three cards x, y and z. A wishes to convey a single bit of information (e.g., whether or not he dyes his hair) to B but not to C, in the presence of both. If A holds x and "guesses" that B holds y, he can make the following announcement: "I hold either x or y." If B responds "so do I," then key is established. If A dyes his hair then he can now say "I dye my hair if my card is x, otherwise I do not." C remains in the dark.

On the other hand if A misguesses (B holds z, not y) B will respond "Sorry; I have neither x nor y;" the key is now blown and A cannot attain his objective. If we define a bit of key to be sufficient for covert communication of a single binary piece of information, then it appears that in this example A has access to, on the average, half a bit of key. Note, by the way, that if C had for some reason revealed his holding, no guessing by A would have been necessary.

With four people dealt thirteen cards each, A could make thirteen guesses of the sort described above, each with success probability one-third (since B has 13 of 39 outstanding cards); hence an average of at least 13/3 bits of key

seems available for covert partnership communication. This is not much to a cryptographer, who needs 23 bits of key to encrypt a telephone number, but to a bridge player the ability to transfer even a single bit of information covertly could be crucial.

Of course, the guessing needed to establish key at the bridge table has to be coded into legal calls. Since there are barely enough of these for sufficient communication to arrive at a good contract, they cannot be wasted solely on the establishment of key. Hence we attempt to establish key only when the attempt simultaneously passes information valuable in the selection of a contract. Key obtained in this manner will be termed active key.

When the opponents have the strong hands we must often be content to listen; frequently their bidding will reveal a piece of information which can be used to establish our key "for free." This passive key can then be used to encrypt defensive signals.

Here is a simple example of an active crypto-convention. A jump raise of partner's opening suit traditionally shows a strong hand with trump support; suppose we require, additionally, either the ace or king of trumps. (With both or neither, some other response, e.g. 3NT, can be employed.) This is useful in itself, since trump quality is important in slam bidding, but it is also an attempt to establish key. If opener is missing both top trumps, he rebids (say) 3NT and key is lost; but otherwise, if interested in slam, he does the following: with the ace of trumps he cue-bids normally, but with the king of trumps he cue-bids a suit in which he lacks control. Responder can tell which by looking at his own top trump, but the opponents have not been tipped off as to the killing opening lead. This could be especially important in duplicate bridge where overtricks are often crucial.

Certain modern conventions which guarantee specific holdings make key establishment an easy second step. An example is "disciplined" weak two-bids, in which an opening two-bid in first or second position shows two of the top three honors in the named suit. Why not have some response (say 2NT) guarantee the missing honor? This could provide a three-way encryption of openers "feature" rebid. Thus the sequence 2 Spades—2NT—3 Hearts could show "either AK of spades and a high heart or AQ of spades and a high diamond or KQ of spades and a high club." Only partner knows for sure!

A variation of a convention sometimes called "Rosenkranz" enables the partner of the overcaller to show the A or K of the overcaller's suit (to indicate a safe lead). Add a way for overcaller to confirm the other card and a scheme for utilizing the key, and "Rosenkranz" becomes "Rosencrypt".

To take advantage of passive key one needs at least two different opening lead agreements (e.g. "fourth best" and "third/fifth") and at least two signalling systems (e.g. "low card encourages" and "high card encourages"). One of the systems is selected for default use when no key is obtained.

Key is obtainable whenever the opponent who eventually becomes declarer gives a reliable count of some quantity in his hand. Examples: declarer answers the Stayman convention, showing four cards of a certain suit, or used the splinter convention, showing one card; declarer shows his aces and kings in a Blackwood reply; declarer reveals his high-card point count within close limits in a notrump sequence; declarer shows out of a suit early in the play. In each case the exposure of the dummy will enable each defender to count the number of the objects in question held by his partner; this becomes key. The opening leader can, for example, use one lead agreement when holding an odd number of "objects" and the other when holding an even number. Partner can "read" the lead as soon as dummy is spread, but hopefully the declarer cannot, until too late in the play.

When key is obtained because declarer has shown out of a suit, it is too late to encrypt the opening lead but perhaps not too late to encrypt some defensive signals. Here a fancy encryption scheme can be used because the defenders may have a lot of reliable key: they, and the only they, know the exact spot-card distribution of the suit in question.

In the following example, taken from [4], East is dealer and neither side is vulnerable.

North
S: 652
H: 1085
D: 74
C: KQJ105

West	East
S: 983	S: QJ4
H: QJ962	H: AK73
D: 1083	D: 952
C: 92	C: A74

South
S: AK107
H: 4
D: AKQJ6
C: 863

East	South	West	North
1NT*	DBL	2H	Pass
Pass	3H	Pass	4C
Pass	4D	Pass	5D(end)

*12-14 points

Playing standard leads and defensive signals, West leads the queen of hearts; declarer ruffs the continuation, draws trumps, and plays the three of clubs toward the table. West is stymied.

If he plays the club deuce, East will think he has three cards in the suit and will win the second round; declarer will take the rest. But if West signals honestly to partner with the nine, declarer will see that he cannot flush out East's ace in two rounds and will be forced to use his club entries to take the double finesse in spades, a play West knows will win.

Playing encrypted signals as described in [2], West has a way out. Hearts, the suit in which declarer has shown out, has become "key" and after trick two declarer cannot tell whether defenders are using normal or upside-down signals. West signals honestly to his partner and declarer must guess.

It should be noted that although passive key is more easily obtained than active key, it must be used with discretion. Some forms are not completely reliable (e.g. Stayman, point-count). Opening leads can be blown and repeated defensive signals present declarer with depths. Worse, it may occasionally happen that the key can be "turned"--declarer determines during the play what system is in use, and takes advantage of deductions concerning the location of cards involved in the key. On balance, though, most forms of passive key are safe and effective. The author leads "attitude" against 3NT with 7 or more points, but fourth-best with 6 or fewer; even though partner cannot always read the lead and declarer can theoretically profit in some circumstances, this convention seems to work nicely.

What is the future of cryptology in bridge? Alan Truscott, bridge columnist of the New York Times, predicted in [1] that it would "open an entirely new field in bridge theory." Further articles [3], [4] and [5] have suggested a variety of other conventions, and we refer readers to these for details. Encryption is already in use by the Taiwanese international bridge team, and is beginning to crop up occasionally in team play. On the other hand, it will be a while before cryptologic conventions are permitted in ordinary tournament play; one such convention was recently turned down in Great Britain, prompting

a scathing editorial in Bridge Magazine. Moreover, all uses of encryption found so far have limited application below the expert level.

As players get better, however, and bidding systems become more accurate, the need for encryption grows; and many more uses for cryptology in bridge may yet be found.

REFERENCES

1. Truscott. Odd Signal Switch. New York Times, Sunday, July 13, 1980.

2. Winkler, P. 1980. Encrypted Signalling. The Bridge World. April: 25-26.

3. Winkler, P. 1980. Knockout. The Bridge World. December: 18-22.

4. Winkler, P. 1981. Cryptologic Techniques in Bidding and Defense, Parts I, II, III, and IV. Bridge Magazine. April: 148-149, May: 186-187, June: 226-227, and July: 12-13.

5. Winkler, P. 1981. My Night at the Cryppie Club. Bridge Magazine. August: 60-63.

Almanac

Friday, May 6, 1983
126th day; 239 to go this year
Sunrise: 5:56; Sunset: 8:24

Today's weather
East wind, rain

TALK ABOUT MISROUTED AND DELAYED MESSAGES!

THE B-21 CRYPTOGRAPH

OSKAR STUERZINGER

In previous issues of Cryptologia [1,2], catalogues and products of "A.B. Cryptograph" Stockholm have been presented.

In the early twenties the Nobel family involved itself in a capital investment and nominated B.C.W. Hagelin, the son of a personal friend of Emanuel Nobel, K.W. Hagelin, the Chief Engineer of the Oil Fields in Baku, as supervisor of that company.

He began his activity in 1921, still running his private company, A.B. Ingenjors-Firman "Teknik", where different electro-mechanical equipment was being developed.

In 1925 rumors reached his office, that the Swedish General Staff had acquired German Enigma machines for studies and was considering the introduction of that equipment into the Armed forces.

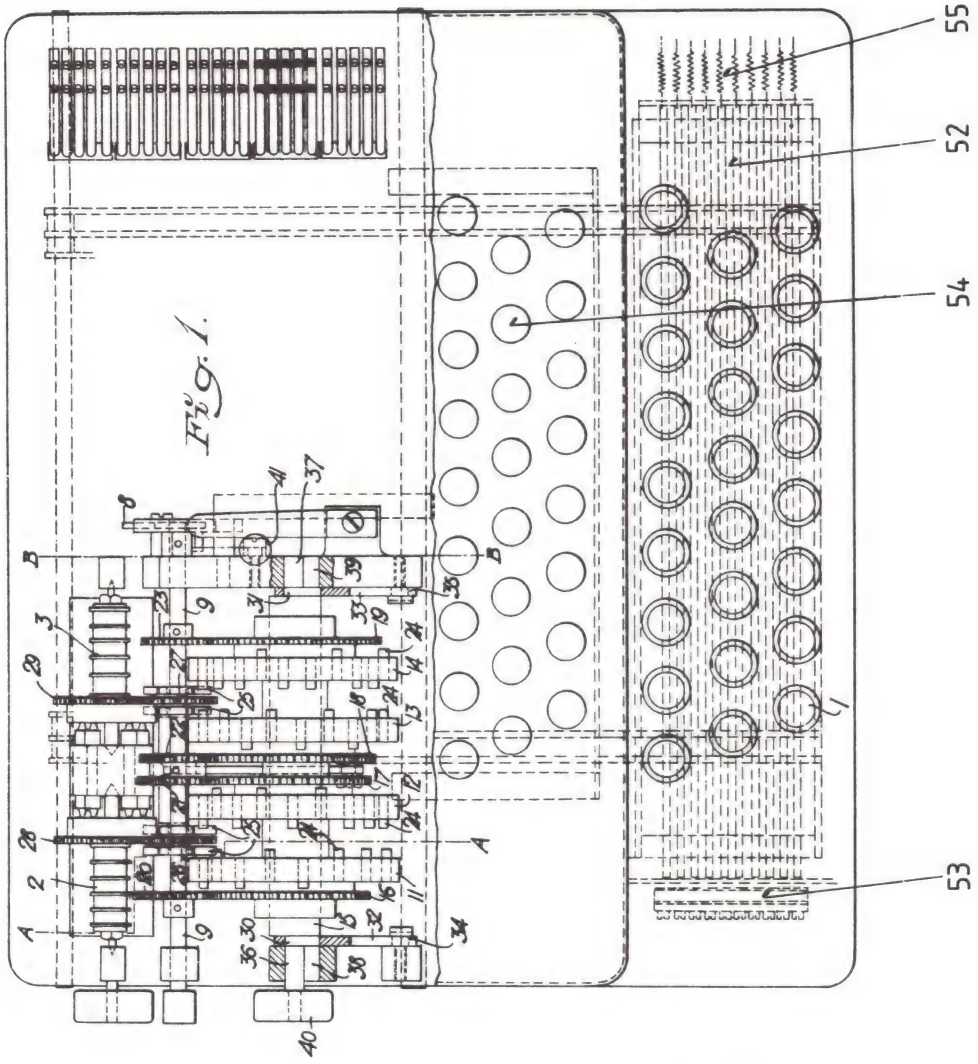
B. Hagelin managed to postpone the final decision, proposing an all-Swedish product. The deal called for a cryptograph similar in shape and operation to the ENIGMA, as this solution--from the practical point of view--had been found very pleasing. Time as well as money was tight; within 6 months a working prototype had to be developed and the money allocated by the Nobels was only Skr 500.—. But, in fact, the development was not starting from scratch. In the past four years, B. Hagelin had acquired enough knowledge from the previous works of A. Damm to be able to create equipment from his own ideas, though still relying on some basic concepts of A. Damm. Thus he was using the Damm rotor as one of the Key generating elements.

It shall be recalled that the idea to use rotors in cryptographic equipment as permutators had apparently been "in the air" since 1918. In fact, Hebern in the USA, Koch in the Netherlands and Scherbius in Germany had suggested its use, independently of each other and patents had been granted to them. (The combination of the ideas of the latter two led to the ENIGMA.) The Damm rotor was, however, somewhat different than the other ones.

Feb. 23, 1932. B. C. W. HAGELIN 1,846,105

CIPHERING APPARATUS

Filed May 28, 1928 2 Sheets-Sheet 1

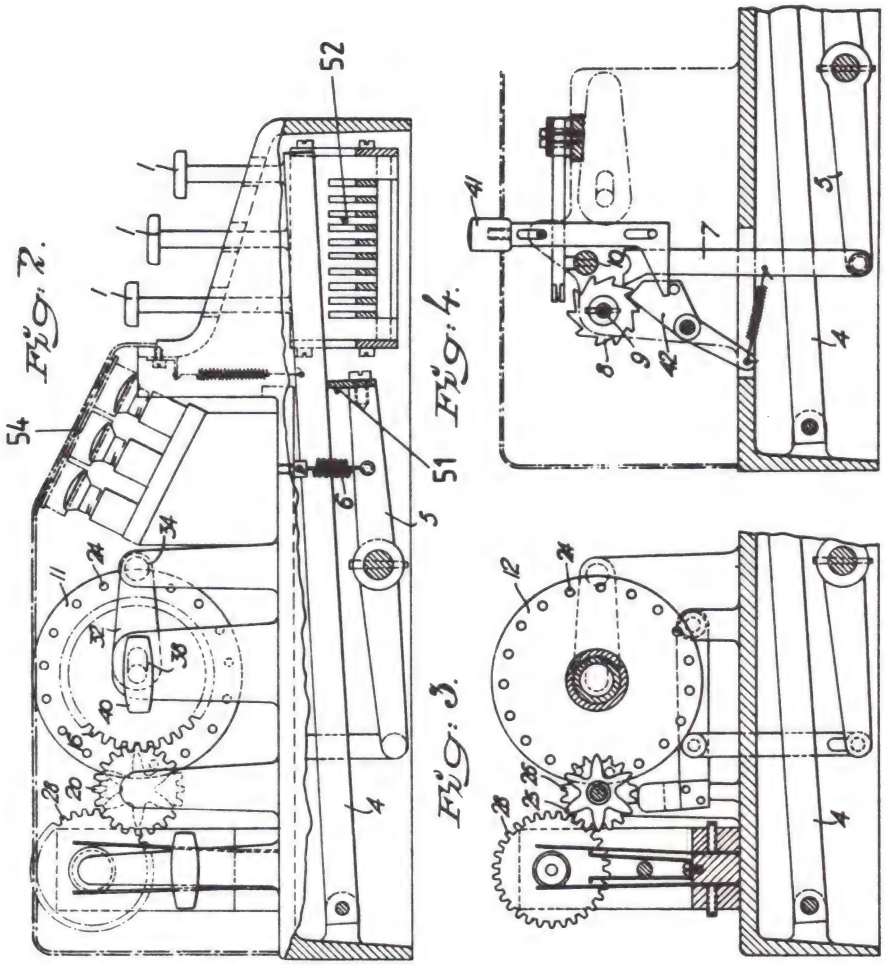


Inventor,
Boris C. W. Hagelin.
By Cleary & Co
Atty.

Feb. 23, 1932. B. C. W. HAGELIN 1,846,105

CIPHERING APPARATUS

Filed May 28, 1928 2 Sheets-Sheet 2



Inventor,
Boris C. W. Hagelin,
By Henry Orth & Co
Atty.

A Hebern or ENIGMA rotor is basically a flat commutator ring, at one side n-single contacts are arranged on a circular surface. They are individually connected to n-contacts of the other side which can move axially under the force of springs. In most cases the rotor is equipped with a toothwheel allowing a step-wise revolution, (Figure 1 shows one possible internal wiring.) Normally a plurality of rotors arranged on a common shaft are connected in series (Figure 2) allowing the production of long key sequences, as each rotor can be moved individually.

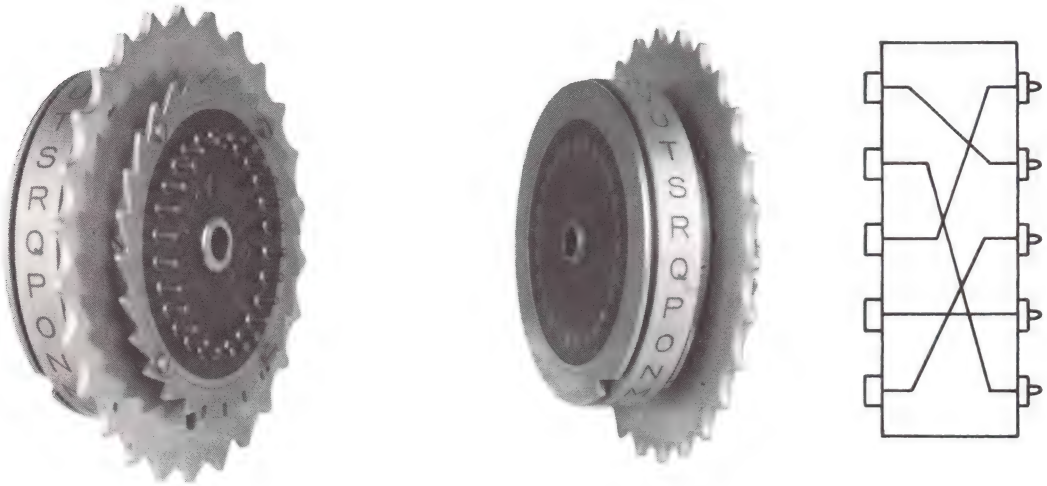


Figure 5. "Standard" Rotor.

The internal criss-cross wiring of the rotors constitutes one of the secret key elements of the machine. There are n! different wiring configurations possible for a rotor, if n is the number of through-connections.

The Damm rotor looks more or less like a telephone stepping switch. One side has circular contact rings linked-up on a string, the other side has contacts distributed on a circular surface, (Figure 3 shows one of all possible internal wirings.) A step-wise revolution provides a similar result as with axial rotors mentioned above. The succession of permutations is, however, not the same!

The Damm rotors had only 5 connections, the basic idea had been the permutation of both—the line as well as the row informations of a 5 x 5 grid—each intersection representing a letter of the latin alphabet (one letter was "sacrificed", normally X having a low frequency in many languages) represented by an incandescent lamp.

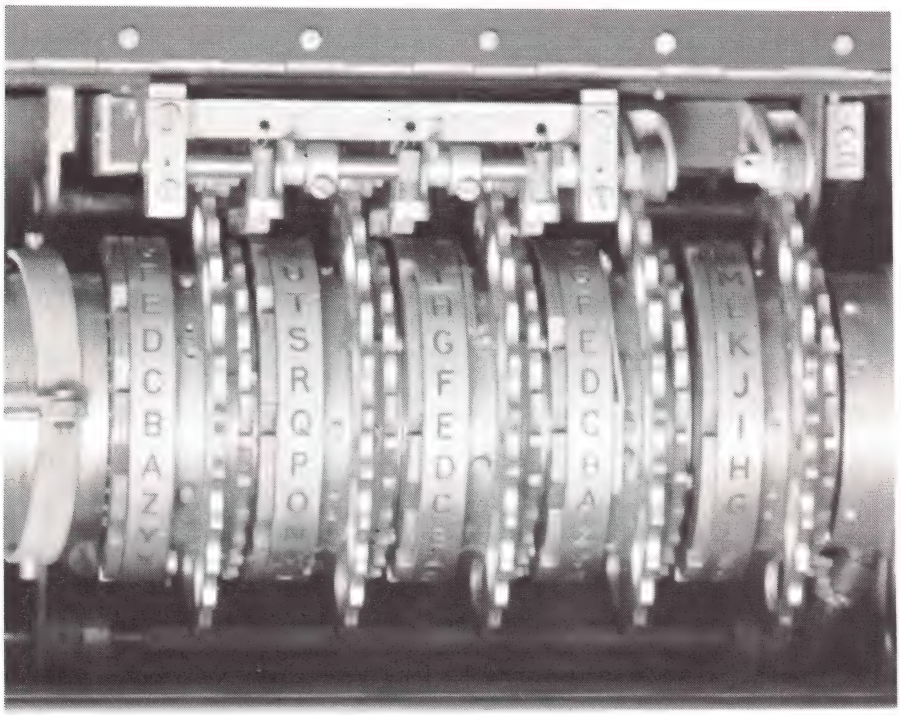


Figure 2. Stack of rotors.

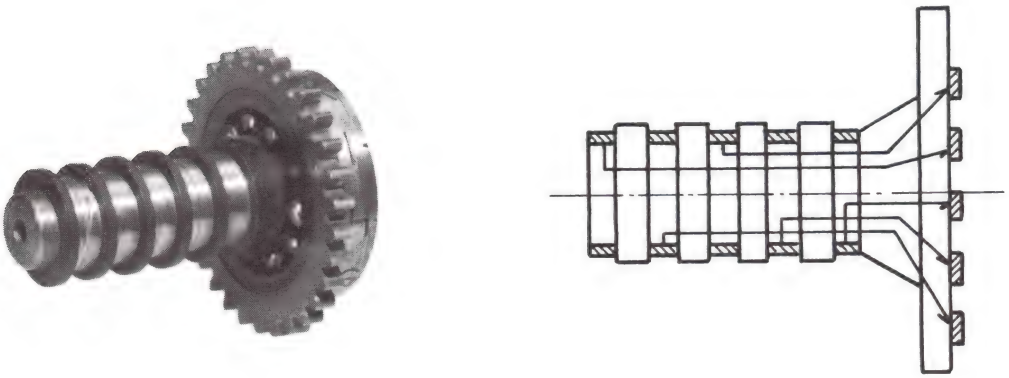


Figure 3. Rotor by A. Damm.

To control the stepping of the rotors, however, B. Hagelin was using a novel system: (Damm had used his famous "chain") pin-wheels. (One pin-wheel had already existed in the fully mechanically A-22 of A. Damm!)

Totally 4 pin-wheels were used, two of each controlling the stepping of one rotor, of which two only were included in the new machine, one for the row informations and one for the line informations.

The machine shall be explained in two steps: one part dealing with the electric circuits, the other with mechanical linkages.

The Electric Layout (Figure 4)

As explained, the concept is based on a 5 x 5 letter alphabet with (diagram Figure 4) each letter represented by a push-button on a keyboard (Primary letter - input -) and a lamp on a display (secondary letter - output .)

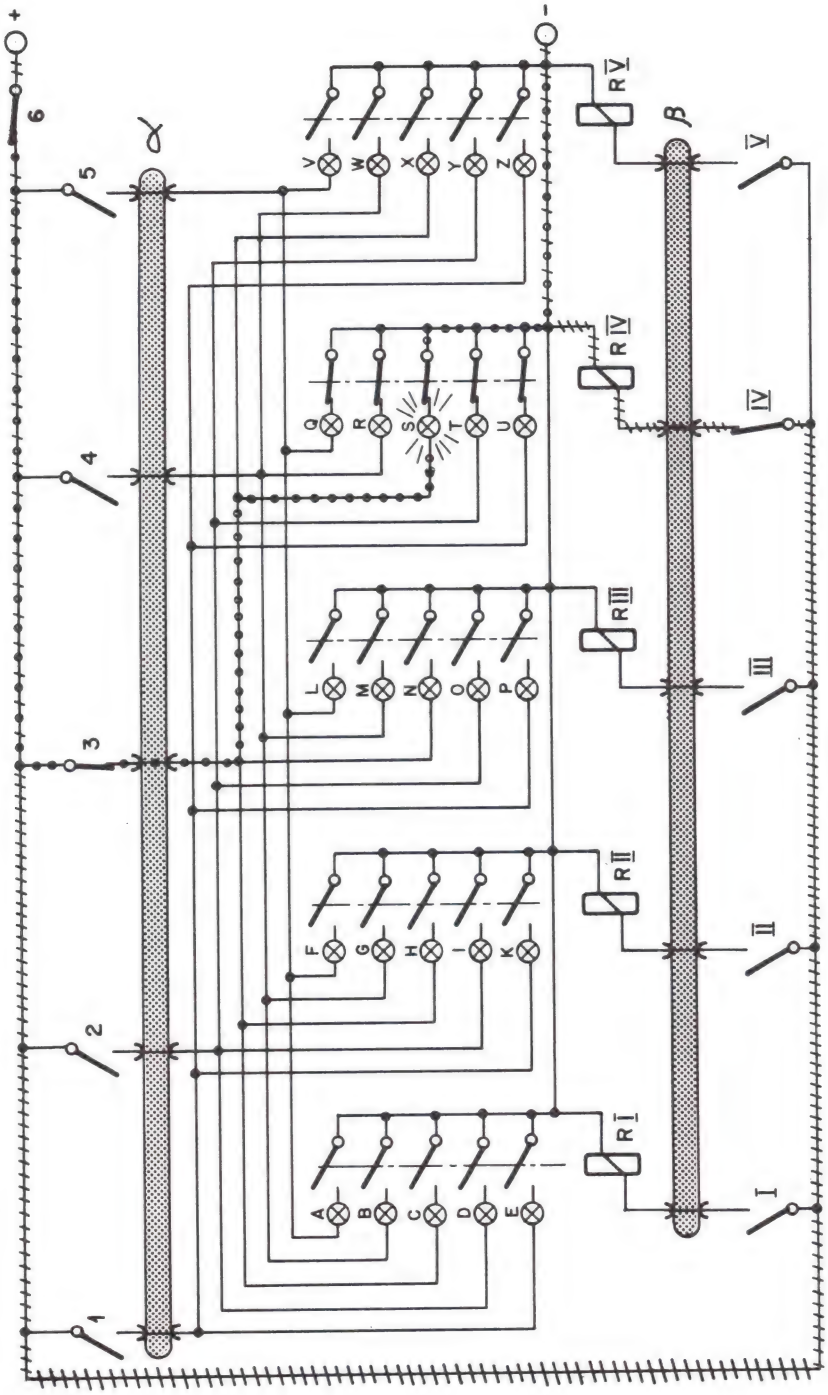
Operating the push-button on the keyboard displaces two of 10 bars in a horizontal movement. Each of these bars closes a contact when activated. The bars are grouped in 2 times 5 ones, the bars 1 - 5 for the lines and the bars I - V for the columns. In Figure 4 bars no. 3 and no. IV are supposed to have been activated. This gives two circuit loops.

One loop goes from + pole through main contact (6) to contact (IV) to rotors (supposed to have a straight - through wiring) to relay (R IV) (which activates its five n.o. contacts) and finally to - pole.

The other loop goes from + pole through main contact (6) to contact (no. 3), rotor α (supposed to be wired straight through) display lamp (S) a contact of activated relay (R.IV) to - pole. Lamp S is lighting-up.

The rotors α and β can be turned step-wise. Naturally, each rotor has its own internal criss-cross wiring from input to output (theoretically 5! = 120 different rotors are possible, this internal wiring being one of the secret "inner key" elements of a machine.) Each rotor has five possible positions. So each line and each row will surely to be connected once in a complete key period.

In the final version the rotors had five contact rings with a total of 10 circular contacts connected internally pair-wise as shown on Figure 8 (giving one of all possible internal wirings.) Also additional permutations of the five row-, and the five line-connections could be made by two rows to plugs, thus giving the possibility to increase the variable elements of a machine without touching the inner wiring of the two rotors.



+++++++ relay loop

●—●—●—● lamp loop

α, β rotors (permutation wheels)
(line 3 and row IV are energized.
in this layout.)

Figure 4.

Basic wiring diagram B-21.

The Mechanical Linkages

Refer to the illustrations (Figure 1 - 4) of US Patent 1,846,105 which had been granted (among patents in other countries) on February 23, 1932, and to Figure 5 and 6.

Figure 5. B-21.

The keyboard comprises 25 levers (4) hinged at the rear and carrying at the front-end, push-buttons (1) marked with the characters like on a typewriter. A rocker bar (51) fixed on rocking levers (5) at the left and right sides is kept at its upper position by two springs (6) hooked into these levers. The bar (51) keeps all 25 character levers (4) in the upper position. Upon striking one of the push-buttons, three operations are performed:

1. The bar (51) is displaced downwards, against the tension of the spring (6.) The left-side lever (5) moves the pawl (7) upwards giving the ratchet wheel (8) a kick of one division (ratchet (42) acting as positioning means.)

2. Two of the 10 contact bars (52) are moved to the left, closing one "row" - and one "line" - contact (53) (contacts 1 - 5 and I - V in Figure 4.) To do so they carry saw-teeth at appropriate places, transforming the vertical movement of a lever (4) in a horizontal movement (Figure 7.)

3. At the extreme position lever (5) closes the contact (6, Figure 4 not shown otherwise), so bringing to illumination one of the 25 indicating lamps of the display (54.)

When released, the character lever (4) is pulled back into its upper rest position by bar (51.) The displaced two contact bars (52) are pulled back by their springs (55.)

Now the movement of the ratchet wheel (8) triggers the following operations:

A. As 4 pinions (20, 21, 22, 23) are fixed on the shaft (9) all along with ratchet wheel (8) the four pin wheels (11, 12, 13, 14) are turned one divisional step by means of the appropriate gear-wheels (16, 17, 18, 19.) The pin wheels have the following divisions: 17, 19, 21, 23 i.e. primary numbers (21 = 3 x 7.) Their pins can have a left or right position.

   For wheels (11) and (13) the right one is the active position, for wheels (12) and (14) it is the left side, which is the active position. On the shaft (9) we have, turning loose, 2 pinions (26,27) which carry on each side a star-wheel (25.) The pinions match with the gear-wheels (28,29) which are solidary with the rotors (2,3) respectively.

B. The rotary movement of one (or two opposite) active pins of one division in the engaging section of the star-wheels (25) brings the rotors (2) resp. (3) through one divisional revolution step. (In fact, the star-wheels are loosely linked to the active pins, unlike a gear-wheel system with interlinked teeth, their angular motion has to be always the equivalent of one divisional step of the rotors, independently of the angular movement of the actuating pin!)

By this means, each stroke of one of the character push-button brings the ciphering system into a new position before the contact (6) is closed, which brings the respective seconadry lamp to glow-up.

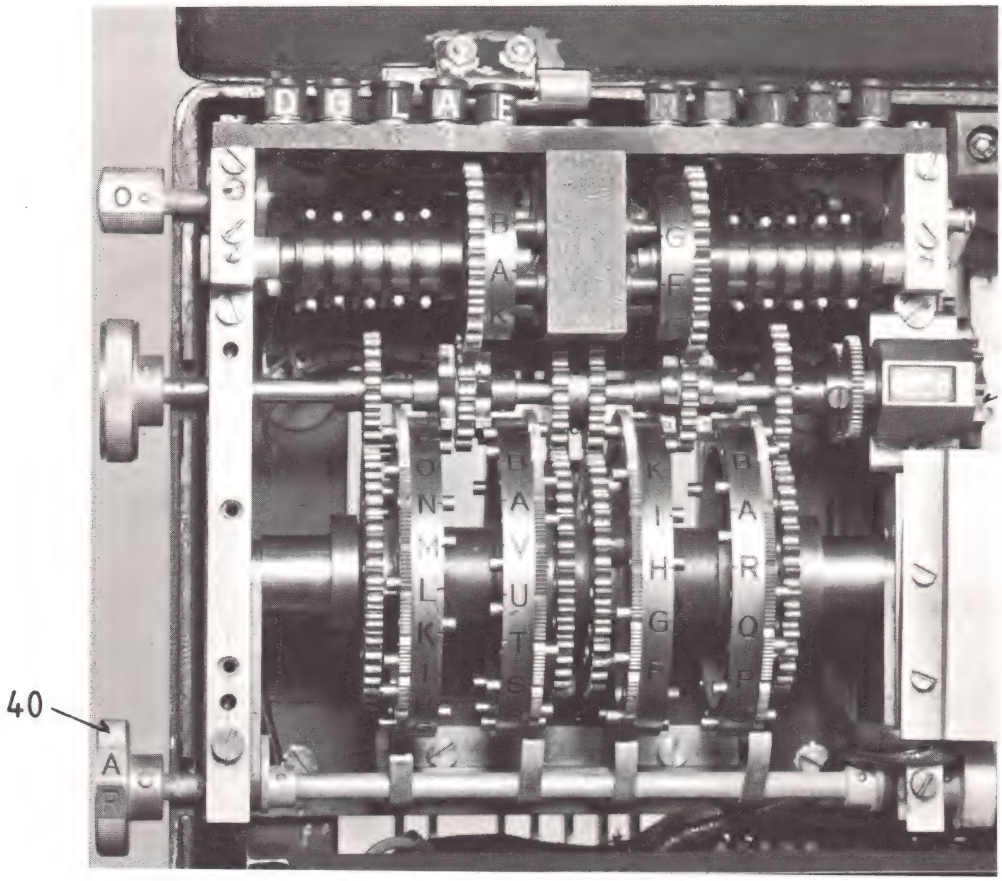


Figure 6. "Key Generator" of B-21.

Not shown in detail are sophisticated electro-mechanical switching systems, which move the brushes of the contact rings of the rotors (2) and (3) so as to make a by-pass circuit (for plain operation) or to inverse the total circuit configuration (for deciphering operation.)

The shaft (15) carrying the 4-pin-wheels can be moved towards the keyboard by means of excentric (40) thus disengaging it from the star-wheels (25) as well as the driving pinions (20, 21, 22, 23.) This allows an independent setting of the 4 pin-wheels as well as the 2 rotors for starting positions, when beginning a new cipher sequence.

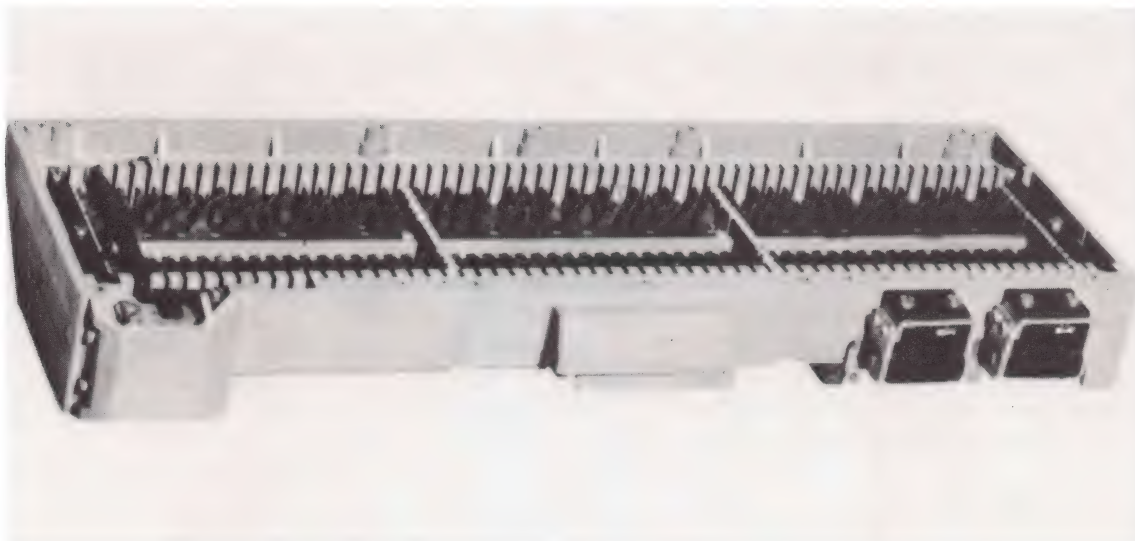


Figure 7. Row of code-bars.

Mathematical Considerations

1. The Rotors

Each rotor has 5 inputs and 2 x 5 outputs. There are, therefore, $(5!)^2$ = 14,400 possible rotor configurations possible. As each machine contains 2 rotors, $((5!)^2)^2$ = 207,260,000 different basic rotor assingments were possible.

2. The Alphabets

As not an independent permutation of the 25 characters takes place, but the two-fold system of "row-families" and "line families", there are only $(5!)^2$ = 14,400 alphabets possible. (In a full single letter permutation system it would be $25! \sim 1.6 \times 10^{25}$.)

As, however, two additional plug rows allow the setting of a basic grid of a alphabet, the total number is also $((5!)^2)^2$ = 207,360,000.

3. The Pin Settings

Each pin-wheel can be set 2^n different pin configurations, this gives a total of $2^{17} \times 2^{19} \times 2^{21} \times 2^{23} \sim 2^{80} \sim 10^{23}$ different total pin settings in a machine.

4. The Key-Period-Length

The period-length of the irregular movement controlling the two rotors (this is important, ENIGMA and HEBERN were using regulars stepping systems for their rotors) is 17 x 19 x 21 x 23 = 156,009.

It is interesting to compare these results with the ENIGMA in its original version (against which this machine had in fact to compete in Stockholm.) The ENIGMA system is not a 26 permutation system but a 2 x 13 system (in effect, to avoid a 26-pole change-over switch for en- respectively deciphering a reflector-wheel was placed at the end of 3 running rotors. Each letter could, therefore, never be represented by itself, but was on the other side naturally linked or "married" to another letter.)

A. The ENIGMA Rotors

Each rotor has 26 criss-cross wirings giving $26! \sim 4 \times 10^{26}$ different rotor configurations. As each machine contains 3 rotors there are $(26!)^3 \sim 6.4 \times 10^{29}$ total basic rotor assignments possible.

B. The ENIGMA Alphabets

The alphabet is, as mentioned a 2 x 13 letter alphabet. We have, therefore, $(13!)^2 \sim (6.2 \times 10^9)^2 \sim 3.6 \times 10^{19}$ different alphabets available. The relative position of the alphabet - rings on the rotors: 26 positions per rotor; 3 rotors: totally $26^3 = 17{,}576$ different settings.

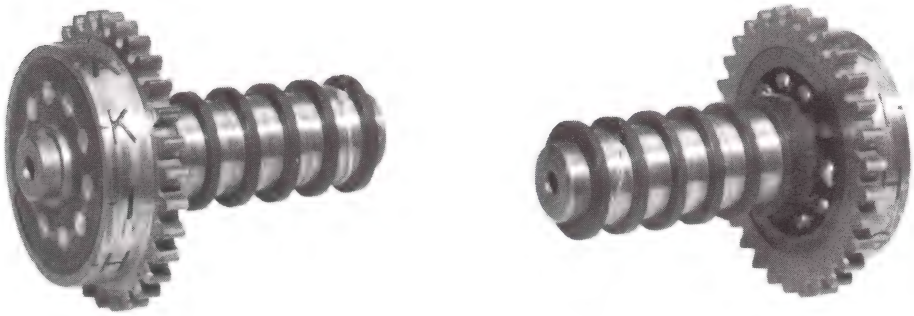
C. The ENIGMA Key Period Length

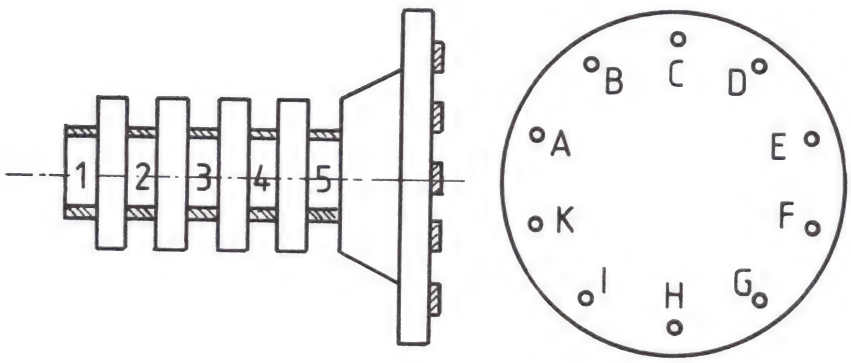
The period length is $26^3 = 17{,}576$ steps.

It can be seen that the advantage of a longer and irregular key period of the B-21 compensates for the smaller alphabet selection. And, most important the field-variable elements the pin setting and the two permutation plug-rows give a tremendous flexibility to that machine against the (original) ENIGMA, where only the alphabet-rings could be moved in the field (exchanging prewired rotors is not considered as a operator's task, this could be performed at both machines and shall be considered as belonging to the basic settings.)

The B-21 was at that time, along with the German ENIGMA, the only cipher machine to be accepted by different defense organizations, both were produced in quantities on an industrial base.

The B-21 was also available in a mains-current version where the operation of a keyboard push-button wash triggering a mains-current fed solenoid-magnet performing the internal stepping movements, so relieving the operator from tedious mechanical handwork.





Internal Wiring :

1 → AF
2 → CD
3 → BI
4 → EH
5 → GK

Figure 8. Final version of Damm - Rotor.

One particular customer, the French authorities were so pleased with the B-21 that they asked for a version with integrated tape printer.

REFERENCES

1. Kruh, L. 1978. A Catalog of Historical Interest - Part I. Cryptologia. 2: 242-253.
2. Kruh, L. 1978. A Catalog of Historical Interest - Part II. Cryptologia. 2: 338-349.

"Oh, how you lied!"

A PUBLIC-KEY CRYPTOSYSTEM BASED UPON EQUATIONS OVER A FINITE FIELD

HUGO BRANDSTROM

ABSTRACT: The present paper describes a public-key cryptological method based upon a relation like $c \equiv m^e$ modulo r where e and r are not known by anyone but the intended receiver of the messages. This is in contrast to the well known method denoted RSA after the introducers Rivest, Shamir and Adleman. Instead of working with very large natural numbers the method as described here works with polynomials over finite fields. How to compute c from m without knowing e and r is described and a very simple case is worked out in some detail

1.0 INTRODUCTION

In 1976 Diffie and Hellman [2] introduced the idea concerning public-key cryptosystems. Since then a number of different concrete methods based upon these ideas have been described [9], [3], [7]. One of the first was presented in [9] by Rivest, Shamir and Adleman and is known as the RSA-method.

In the present paper a method based upon the same basic ideas is described which has some resemblance to the RSA-method. They differ, however, in one essential respect. While the RSA-method operates upon natural numbers our method operates upon polynomials with coefficients belonging to a finite field especially the binary field.

Both the ring of natural numbers and the ring of polynomials are Euclidian rings which implies that each element in the ring can be factorized into prime elements (prime-numbers and irreducible polynomials respectively). The encryption algorithm is in both systems defined by a relation of the following type

$$c \equiv m^e \text{ modulo } r \qquad (1)$$

where m is a ring element representing the plain text, c is a ring element representing the encrypted message and e is a natural number.

In the RSA-method r is the product of two large prime numbers p and q and decryption is realized by

$$m \equiv c^d \text{ modulo } r \qquad (2)$$

where d is a solution of $d \cdot e \equiv 1$ modulo the least common multiple of p-1 and q-1.

The numbers r and e are supposed to be available to everyone. But the factors p and q are kept secret to all but the receiver of the encrypted messages.

The difficulty in cracking the messages is based upon the well known fact that it is a very difficult task to resolve large numbers ($\simeq 10^{200}$) into their prime factors. This implies that although r is known, p and q remain unknown to a cracker. Therefore he cannot determine the value of d.

In the alternative method which will be described in the following pages, r is a primitive polynomial and both r and e are unknown for everyone except the receiver A of the encrypted message c.

One drawback with this method is, however, that we lose the possibility to generate digital signatures.

The security of the proposed cryptological method is discussed and this discussion is based upon a special polynomial algebra which seems to be the right tool for this analysis.

2.0 THE ALTERNATIVE METHOD

As mentioned earlier this method works with polynomials with coefficients belonging to a finite field. If we use the ring of integers as the domain of the coefficients then the residue classes modulo an irreducible polynom p(x) of degree m would not be a finite set and the elements $c_k \equiv m^k$ modulo p(x) for k = 0,1,2,..., would in the general case generate an infinite semigroup which implies that a decryption by means of a relation

$$m \equiv c_e^d \text{ modulo } p(x)$$

is impossible. When the coefficients of the polynomials belong to a finite field however the situation is different and quite similar to the case of the RSA-method.

In the following we limit our treatment to the case when the coefficients belong to the binary field. Let the user A choose a primitive polynomial $p(x)$ of degree m. We chose $p(x) = 1 + x + x^4$ ($m = 4$) as an illustrative example. The values of different constants in this example are given within parentheses. The set of residue classes modulo $p(x)$ is a finite field isomorphic to the Galois-field $GF(2^m)$.

In the second column in the appendix it is shown how x^n passes through all the elements in this field (with $p(x) = 1 + x + x^4$) when n goes from 0 to 14.

Speaking about a polynomial field of this kind we let K denote the field to which the polynomial coefficients belong. The binary field is denoted by K_0. The corresponding polynomial field is named $K(x;p)$ where $p = p(x)$ is the primitive polynomial. Thus the polynomial field whose non-zero elements are given in the second column in the appendix is denoted by $K_0\ (x;1 + x + x^4)$. In the third column in the same table the corresponding elements in $K(x;2 + x + x^2)$ are given where $K \sim GF(4)$ and 2 is a primitive element in K. These two polynomial fields are both isomorphic to GF(16). We let the number of elements in K be $|K| = k$.

Also let elements from the Greek alphabet (with or without subscript) denote variables with domain K. Such a variable α is supposed to satisfy the relation $\alpha^k = \alpha$.

With these assumptions $F(x) = \alpha + \beta x + \gamma x^2 + \delta x^3$ becomes an element in $K_0(x; 1 + x + x^4)$ as soon as α β, γ, δ have been given values in K_0. We say that $F(x)$ is a polynomial variable with values in $K_0(x; 1 + x + x^4)$.

Let $q = 2^m - 1$ (= 15) and suppose that the user A besides $p(x)$ also chooses an exponent e (= 7) which is relatively prime to q, i.e., the largest common divisor of e and q is 1. Before we proceed with the specification of the cryptological algorithm we want to work through the example chosen where $K = K_0$ and $p(x) = 1 + x + x^4$.

This example is not representative in concrete data-security connections where the degree m of $p(x)$ is supposed to be about 10 times as large.

2.1 Example

Let $F(x) = \alpha + \beta x + \gamma x^2 + \delta x^3$ be a polynomial variable with values in $K_0(x; 1 + x + x^4)$. Using the table in appendix A we will determine the polynomial functions $\varphi_v(\underline{\alpha})$ of the vector $\underline{\alpha} = (\alpha, \beta, \gamma, \delta)$ given by the relation

$$F(X)^e = F(x)^7 = \varphi_0 + \varphi_1 \cdot x + \varphi_2 \cdot x^2 + \varphi_3 \cdot x^3$$

In this example we have exploited the facts that $F(e)^7$ is the inverse of $F(e)^8 = \alpha + \beta + (\gamma + \delta)x + \beta x^2 + \delta x^3$ to get a system of linear equations in $\varphi = (\varphi_0, \varphi_1, \varphi_2, \varphi_3)$ whose determinant we know to be 1. Its solution is

$$\varphi_0 = \begin{vmatrix} \alpha+\beta+\delta & \beta+\delta & \beta+\gamma+\delta \\ \gamma+\delta & \alpha+\beta+\delta & \beta+\delta \\ \beta & \gamma+\delta & \alpha+\beta+\delta \end{vmatrix} \quad \varphi_1 = \begin{vmatrix} \gamma+\delta & \beta+\delta & \beta+\gamma+\delta \\ \beta & \alpha+\beta+\delta & \beta+\delta \\ \delta & \beta+\delta & \alpha+\beta+\delta \end{vmatrix}$$

$$\varphi_2 = \begin{vmatrix} \gamma+\delta & \alpha+\beta+\delta & \beta+\gamma+\delta \\ \beta & \gamma+\delta & \beta+\delta \\ \delta & \beta & \alpha+\beta+\delta \end{vmatrix} \quad \varphi_3 = \begin{vmatrix} \gamma+\delta & \alpha+\beta+\delta & \beta+\delta \\ \beta & \gamma+\delta & \alpha+\beta+\delta \\ \delta & \beta & \gamma+\delta \end{vmatrix}$$

Written in this way the polynomial functions φ_v are seen to be of degree at most three and they unveil the fact that e is one of the numbers $2^i + 2^j + 2^k$, $0 \leq i < j < k \leq 3$ since $_{F(x)}2^i$ is linear in $\underline{a}$ for all i.

In the cryptological method which will be described in section 2.2 the user A generates a program for computing the values of the polynomial functions $\varphi_v(\alpha)$ for every binary number $\underline{a}$ which $\underline{\alpha}$ assumes when its components α β, γ and δ assume values in K_o. This program is supposed to be accessible for everyone. A weakness in the cryptological system arises however if the number of bits $|\underline{a}|$ in $\underline{a}$ agrees with the number of polynomials φ_v. A cracker can then conclude that the degree m of p(x) is $m = |\underline{a}|$ (= 4).

This weakness can however be reduced essentially by A if he takes the two following steps.

i. A only makes use of a subspace of the m-dimensional space K(x;p(x)) over K. He may for example say that only the variables α, β, and γ are relevant and stipulate that δ has a prescribed value. If $\delta = 0$ we get

$$\begin{aligned} \varphi_0 &= \alpha + \beta + \gamma + \alpha\beta + \alpha\beta\gamma & \varphi_1 &= \beta + \alpha + \alpha\gamma \\ \varphi_2 &= \alpha\beta + \beta\gamma + \alpha\gamma & \varphi_3 &= \beta + \gamma \end{aligned} \tag{3}$$

ii. A introduces redundancy by generating additional polynomials $\varphi_v(\underline{\alpha})$. A redundant polynomial $\varphi_4(\underline{\alpha})$ is for example

$$\varphi_4 = \alpha + \gamma + \alpha\beta\gamma \tag{4}$$

Using these polynomials A can guarantee that a cracker only knows that the degree m of p satisfies the relations $3 \leq m \leq 5$.

The reduction in i. is just the reason why the possibility of digital signatures is lost.

We are now ready to describe the cryptological method in general terms.

2.2 Cryptologic procedure

We continue to work with $K = K_o$. The user A takes the following eight preliminary steps.

1. Chooses a primitive polynomial $p(x)$ with coefficients in K_o and of degree m ($q = 2^m - 1$).

2. Chooses a polynomial $h(x)$ in $K_o(x;p(x))$

3. Chooses a subspace S of polynomials in $K_o(x;p(x))$ determined by n natural numbers i_v where $0 \leq i_1 < i_2 \ldots < i_n < m$ and $n < m$ and by the condition that $Q(x) = \alpha_1 \cdot x^{i_1} + \alpha_2 \cdot x^{i_2} + \ldots + \alpha_n \cdot x^{i_n}$ becomes an element in S when the coefficients assume values in K_o. We let $F(x) = Q(x) + h(x)$.

4. Chooses e in such a way that the largest common divisor (1. c. d.) of e and q is 1.

5. Determines the polynomials $\varphi_v(\underline{\alpha})$ where $\underline{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $v = 0, 1, 2, \ldots, M$, $M \geq m-1$, by the conditions

$$G(x) \equiv \sum_{v=0}^{m-1} \varphi_v(\underline{\alpha}) \cdot x^v \equiv F(x)^e \text{ modulo } p(x)$$

and $\varphi_v(\underline{\alpha})$ $v = m, m+1, \ldots, M$ are arbitrary.

6. Chooses a permutation π of the set of numbers $(0, 1, \ldots, M)$ and puts $\varphi_v(\underline{\alpha}) = \varphi_{\pi(v)}(\underline{\alpha})$ for $v = 0, 1, 2, \ldots, M$.

7. Produces a data-program for computing the values $\theta_v(\underline{a})$ for all $\underline{a} \in K^n$ and $v = 0, 1, \ldots, M$. We will call this program the key program.

8. Puts the key program in a public file under a name AN chosen.

Everyone who wants to communicate with A using this cryptosystem fetches the key program AN from the public file and for each n-dimensional binary vector $\underline{a} = (a_1, \ldots, a_n)$ which he wants to transmit to A he computes the M-1-

dimensional binary vector $\underline{b} = (b_0, b_1, \ldots, b_M)$ where $b_v = \theta_v(\underline{a})$. This vector is transmitted to A.

The receiver A generates the m-dimensional binary vector $\underline{c} = (c_0, c_1, \ldots, c_{m-1})$ from $\underline{b}$ by means of the permutation π defined under 6, above using the relation

$$c_v = b_{\pi^{-1}(v)} = \theta_{\pi^{-1}(v)}(\underline{a}) = \varphi_v(\underline{a}) \qquad v = 0,1,\ldots,m-1$$

The element $g(x) = \sum_{v=0}^{m-1} c_v x^v$ in $K_o(x;p(x))$ satisfies

$$g(x) \equiv f(x)^e \text{ modulo } p(x) \tag{5}$$

where

$$f(x) = \sum_{v=1}^{n} a_v x^{i_v} + h(x) \tag{6}$$

Comparing (5) with (1) in the introduction we see that we have reached our aim. A has not for anyone disclosed the primitive polynomial p(x) or the exponent e. Other people only know that the degree m of p(x) satisfies the relations $n \leq m \leq M+1$ where n and M are publicly known and $n < M$.

Also no one but A knows which M-m+1 components in the vector $\underline{b}$ are redundant since only A knows the permutation π. Furthermore the polynomial h(x) and the integers i_v are unknown by all but A.

The set $\{\theta_v\}$ of M+1 polynomials is the only publicly known fact (besides that $n \leq m \leq M+1$) about the system and the possibilities to determine the secret parts of it from this information seem to be quite small if there are any possibilities at all.

Only A who knows e and q can evaluate d from the relation

$$d \cdot e \equiv 1 \text{ modulo } q \text{ (if } q = 15 \text{ and } e = 7 \text{ then } d = 13).$$

A then gets

$$f(x) \equiv g(x)^d \text{ modulo } p(x). \tag{7}$$

Error in the transmission may be detected from the condition that the only values of j in

$$f(x) - h(x) = \sum_{j=0}^{m-1} a'_j x^j$$

for which a'_j may differ from 0 are $j=i_1, i_2, \ldots, i_n$ if no errors occur.

3.0 CRYPTOLOGICAL SECURITY

The security of the cryptological method as described in the last section rests upon the difficulties to solve the equations (in $\underline{a}$)

$$\theta_v(\underline{a}) = b_v \quad v = 0, 1, 2, \ldots, M. \tag{8}$$

A cracker is of course supposed to know that these equations have been determined by means of multiplications within a finite polynomial field but if he does not know much about the degree of this finite field the knowledge he has a priori seems to be of limited value.

The cracker may have some help of the knowledge that $n \leq m \leq M$ since he then knows that $K_o(x;p(x))$ is isomorphic to a subfield of $GF(2^N)$ where $N = M/(n-1)!$ but N is a relatively large number and at present it seems to be difficult to make use of this.

In order to discuss the equations (8) we write them in the following way:

$$\varphi_v(\underline{a}) = c_v \quad v = 0,1,\ldots,m-1,m,\ldots,M \tag{9}$$

where $c_v = b_{\pi^{-1}(v)}$.

The polynomial g(x) in (5) only contents the coefficients c_v where $0 \leq v < m$. We may conclude that the m first equations in (9) give a unique solution of $\underline{a}$.

One way of attack to this system of equations will be discussed here since it at the same time indicates some of the most essential rules which A has to follow when choosing the redundant functions φ_v, $m \leq v \leq M$ in order not to make the crackers job more easy than necessary. The discussion is based upon the algebra of polynomials which will be introduced in the next section.

3.1 The algebra of polynomials

In the present section we start with a field K which does not need to be K_o and as before let $k = |K|$ = number of elements in K. The variables $\underline{\alpha}_v$, $v = 1, 2, 3, \ldots, n$, are still supposed to satisfy the condition $\alpha_v^k = \alpha_v$ but in addition we consider them as basis vectors of a n-dimensional vector space V over k. The algebra P of polynomials is defined by means of the following set of basis vectors

$$\alpha_1^{v_1} \cdot \alpha_2^{v_2} \cdot \ldots \cdot \alpha_n^{v_n} \quad v_j \in \{0, 1, 2, \ldots, k-1\}$$

where we define $\alpha^0 = 1 \in K$ and of course $\alpha_i \cdot \alpha_j = \alpha_j \cdot \alpha_i$ for all i and j.

As a vector space over K this algebra has dimension $d = k^n$. P is a graded algebra

$$P = V_0 \oplus V_1 \oplus \ldots \oplus V_{d_0} \qquad d_0 = n(k-1)$$

where $V_0 = K$, $V_1 = V$ and the set of elements $\alpha_1^{v_1} \cdot \alpha_2^{v_2} \ldots \cdot \alpha_n^{v_n}$ where $v_1 + v_2 + \ldots + v_n = j$ is a basis for V_j. We put

$$P_j = V_0 \oplus V_1 \oplus \ldots \oplus V_j \qquad j \in \{0, 1, \ldots, d_0\}$$

From now on we suppose that $K = K_o$ and $k = 2$. Then all the polynomials φ_v are elements in P. According to the relation (7) we know that the elements α_v may be expressed as polynomials with the nonredundant elements φ_v, $v = 0,1,2,\ldots, m-1$ as arguments. Therefore the set $\{\varphi_v \mid v = 0, 1, \ldots, m-1\}$ is a set of generators in P.

Let U be the smallest subspace of the vector space P which contains the set $\{\varphi_v \mid v = 0, 1, 2, \ldots, m-1\}$. We call it the nonredundant space. Also let R be the smallest vector subspace of P which contains set $\{\varphi_v \mid v = 0,1,..,M\}$. Since the set $\{\theta_v \mid v = 0, 1, \ldots, M\}$ is identical with the set $\{\varphi_v = \theta_\pi^{-1}(v) \mid v = 0, 1, \ldots, M\}$ the cracker may know R but only A knows U.

Two vector subspaces of special interest in the analysis of resistivity to cracking are $U_1 = U \cap P_1$ and $R_1 = R \cap P_1$. We know that

$$U_1 \subseteq R_1 \subseteq P_1$$

We call U_1 the linear nonredundant space and R_1 the linear cryptospace.

Let $\dim U_1 = u$, $\dim R_1 = r$. Then $u \leq r \leq n+1$.

Also let $\underline{\xi} = (\xi_1, \xi_2, \ldots, \xi_r)$ be a basis in R_1 and let $\underline{\theta} = (\theta_0, \theta_1, \ldots, \theta_M)$. Since $R_1 \subseteq R$ there is an M x r matrix T with elements in K_o such that

$$\underline{\xi} = \underline{\theta} \cdot T \tag{10}$$

We suppose that the cracker has found such a matrix T which maps R onto R_1.

Also since $R_1 \subseteq P_1$ we have

$$\underline{\xi} = (1, \alpha_1, \alpha_2, \ldots, \alpha_n) \cdot \eta \tag{11}$$

where S is an (n+1) x r matrix over K_o.

In (10) $\underline{\theta}$ is now replaced by $\underline{b} = (b_0, b_1, \ldots, b_M)$. The value of $\underline{\xi}$ becomes $\underline{r} = (r_1, r_2, \ldots, r_r)$ where

$$\underline{r} = \underline{b} \cdot T \tag{12}$$

which we put into (11) and get the following linear equations in the values a_v of α_v

$$(1, a_1, a_2, \ldots, a_n) \cdot S = r \tag{13}$$

The range of S is at most $r \leq n+1$. If it is n+1 then the plain text message $\underline{a} = (a_1, a_2, \ldots, a_n)$ may be computed by solving a system of linear equations over the binary field.

If $r \leq n$ on the other hand and if S minus the first row has the same range then r of the n unknowns a_v may be expressed as linear functions of the other n+1−r unknowns. Substituting these linear functions in the polynomials $\theta_v(\underline{a})$ these polynomials reduce to M+1 polynomials with n+1−r unknowns.

The user A wants to reduce the dimension r of R_1 as much as possible by choosing the redundant polynomials φ_v $v = m, m+1, \ldots, M$ in a suitable way. But since $U_1 \subseteq R_1$ the dimension $r \geq u$.

By choosing the redundant polynomials within the nonredundant space U however A can guarantee that $R_1 = U_1$. This is also the case if all the redundant elements φ_v $m \leq v \leq M$ have nondisappearing nonlinear components which are mutually linearly independent and also linearly independent of the nonlinear components in the nonredundant elements.

As an illustration we consider the polynomials in (3) and (4). They may be transformed into the following linearly independent elements

$$\tau_0 = \varphi_0 + \varphi_4 = \beta + \alpha \cdot \beta$$

$$\tau_1 = \varphi_0 + \varphi_1 + \varphi_4 = \alpha \cdot \gamma$$

$$\tau_2 = \varphi_0 + \varphi_1 + \varphi_2 + \varphi_4 = \beta + \beta\gamma$$

$$\tau_3 = \varphi_3 = \beta + \gamma$$

$$\tau_4 = \varphi_4 = \alpha + \gamma + \alpha\beta\gamma$$

We observe that all the nonlinear components $\alpha\beta$, $\alpha\gamma$, $\beta\gamma$ and $\alpha\beta\gamma$ of the elements τ_v are mutually linearly independent and R_1 is one dimensional $R_1 = K_0 \cdot \tau_3$. Since $\tau_3 \varepsilon U_1$ we get $R_1 = U_1$. If t_v is the actual value of τ_v for $v = 0, 1, \ldots, 4$ then substituting the value of $\tau_3 + \beta$ for the value of γ we get the following system of equations

$$b + ab = t_0,\quad b + t_3 a = t_1,\quad t_3 b = t_2,\quad b + a + t_3 ab = t_3 + t_4,\quad b + c = t_3 \qquad (14)$$

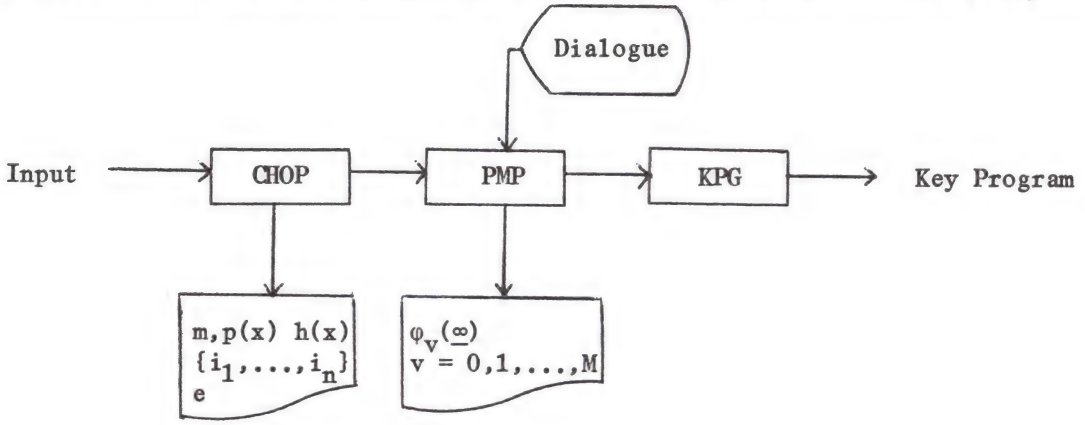
where a, b, and c are the solutions of α, β, and γ respectively.

In (14) we have five equations in three unknowns. If the vector $\underline{b} = (b_0, b_1, \ldots, b_M)$ has been disturbed by noise on its way to the cracker then this system of equations may be inconsistent. If this is not the case the solution in a, b, and c is unique and easily worked out in this simple example. But with increasing values of n, m, and M-n the complexity of the cracking problem increases rapidly. As seen in Section 3.1 the choice of value of e also has an effect upon this complexity. The present paper is not the right place to treat the nonlinear cases in more details.

Also we do not describe the particular program which should be needed in assisting A when developing the key program. This program which is discussed in [1] is built around three subroutines CHOP, PMP and KPG respectively where CHOP chooses by random the integers and polynomials which are given in the first four points in Section 3.2, PMP a polynomial manipulation program generates polynomial functions $\varphi_v(\underline{\alpha})$ in point 5 and KPG generates the key program in point 7. In the next chapter we account for the different steps when using this main program to generate the key program.

4 EXECUTING THE MAIN PROGRAM

The execution of the main program proceeds according to the following figure.



At the start the main program accepts as input a natural number arbitrarily chosen by A in order to put a pseudo-random number generator in a start position. As information to A and nobody else the subroutine CHOP outputs m, p(x), h(x), $(i_1,\ldots,i_n)$ and e which have been generated by means of a pseudo-random generator. These entities are also the inputs to the subroutine PMP which begins by generating text strings containing the polynomials $\varphi_v(\underline{\alpha})$ v = 0,1,2,...,m-1. These polynomials are presented in dialogue to the operator A who helps PMP in generating the polynomials $\varphi_v(\underline{\alpha})$ v = m,m+1,...,M. All these M+1 polynomials are also printed out as information to A. They are also inputs to KPG which delivers the key program as output.

REFERENCES

1. Brändström, H. 1981. Polynomials over finite fields as means to generate public-key cryptosystems. Report RTA U10001. Solna, Sweden: Teleplan. Oct.

2. Diffie, W. and M. E. Hellman. 1976. New directions in cryptography. IEEE Trans Inform Theory. 644-654.

3. Diffie W., and M. E. Hellman. 1979. Privacy and authentication: An introduction to cryptography. Proc of the IEEE. 67: 397-427.

4. Herlestam, T. 1978. Critical remarks on some public-key cryptosystems. BIT. 18: 493-496.

5. Herlestam, T. 1979. Algebra med tillämpningar pa kryptologi m m. Lecture notes. The Lund Institute of Technology. Stockholm.

6. Johannesson, R. 1981. Nagot om kryptering. Lecture Notes. The Lund Institute of Technology. Stockholm.

7. Merkle, R. and M. E. Hellman. 1978. Hiding information and signatures in trap door knapsacks. IEEE Trans Inform Theory. 525-530.

8. Riesel, H. 1978. En teori för kryptering med fallucksfunktioner. Lecture notes. Royal Institute of Technology. Stockholm.

9. Rivest, R. L., A. Shamir, and L. Adleman. 1978. On digital signatures and public-key cryptosystems. Commun ACM. 21: 120-126.

APPENDIX

The residue classes of:

1. Polynomials over the binary field modulo $p(x) = 1 + x + x^4$.

2. Polynomials over the field GF(4) modulo $q(x) = 2 + x + x^2$, where GF(4) = {0, 1, 2, 3,}. Here 2 and 3 are the roots of $t^2 + t + 1 = 0$. Both these polynomial fields are isomorphic to GF(16).

n	x^n modulo $(1 + x + x^4)$	x^n modulo $(2 + x + x^2)$
0	1	1
1	x	x
2	x^2	$2 + x$
3	x^3	$2 + 3x$
4	$1 + x$	$1 + x$
5	$x + x^2$	2
6	$x^2 + x^3$	$2x$
7	$1 + x + x^3$	$3 + 2x$
8	$1 + x^2$	$3 + x$
9	$x + x^3$	$2 + 2x$
10	$1 + x + x^2$	3
11	$x + x^2 + x^3$	$3x$
12	$1 + x + x^2 + x^3$	$1 + 3x$
13	$1 + x^2 + x^3$	$1 + 2x$
14	$1 + x^3$	$3 + 3x$
15	1	1

ROTERM
A MICROPROCESSOR BASED CIPHER TERMINAL SYSTEM

DANIEL WOLF

ABSTRACT: Microprocessors are playing an increasingly important role in cryptographic systems. ROTERM is an implementation of a cipher terminal using an inexpensive microcomputer system. ROTERM behaves like a mechanical rotor system of eight rotors with 96 elements each. Control features have been implemented in ROTERM which permit keyboard and/or remote control of the encipherment and decipherment of ASCII character strings. Examples are given demonstrating the use of ROTERM in user-user communications as well as user-electronic mail system posting and reading of messages.

There have appeared in these pages a number of articles on implementations of cryptographic systems using programmable calculators. These articles, along with the reviews of state of the art cipher machines emphasize the impact of microelectronics on modern cryptography. This article develops a high speed cryptographic system using a general purpose microcomputer. The marketplace now offers several personal computers suitable for cryptographic research. Personal computers based on popular microprocessors are, in some important ways, much more powerful than programmable calculators. They also permit more than one cipher system to be used, in contrast with the dedicated cipher machines. Their third advantage is that many suitable computers are much less costly than the cipher-only machines. They are sometimes less expensive than programmable calculators.

The design goals for the system presented here are:

1. Moderate to high security
2. Speed—capability for encryption and decryption at 30 characters per second for full duplex 300 baud terminal telecommunications
3. Memory requirement less than 8192 bytes
4. Simple, user-friendly operation
5. Total system hardware cost less than $500.00.

The cipher system used is a simulated rotor machine with eight alphabet wheels, each alphabet containing the 96 printable ASCII characters. It is capable of a poly-alphabetic substitution at 300 baud. The rotor software is embedded in a "dumb" terminal program, enabling the microcomputer to function as a full-duplex telecommunications terminal in either clear or cipher modes.

The computer hardware used is an Ohio Scientific Superboard II/Challenger 1. It has the following properties:

1. 6502 microprocessor, found in many other popular personal computers, operation at 1 MHZ
2. 8K random access user memory
3. 8K BASIC language interpreter program in read only memory
4. 300 baud cassette tape/RS-232 serial input/output port with cables
5. Video display generator of 24 lines of 24 characters each, with cable
6. 53 key full typewriter keyboard
7. Built-in monitor software for serial I/O, video display, and keyboard read operation
8. All on a single printed circuit card, operating from a single five volt, three ampere supply

The ROTERM cipher system consists of about 500 bytes of 6502 machine language instructions plus a BASIC program of about 500 bytes. An additional 2048 bytes are set aside as an array space for the rotor "wheels." All of the software is conveniently stored on a cassette tape. It can be loaded into the system in less than five minutes.

The ROTERM Wheels

Each rotor wheel is a 96 byte array, stored in contiguous bytes of memory. The placement (see memory map in Table 1) of the wheels in memory is chosen to simplify the machine instructions necessary for encoding, decoding, wheel rotation, etc. As in a mechanical rotor system, each wheel represents a permutation of the alphabet employed. Ciphering takes a plaintext character "through the wheels" resulting in a ciphertext character. Deciphering runs the cipher character through the wheels in reverse to yield the plaintext character. After each character is processed, the wheels are rotated in such a way that the second wheel makes one forward step for each complete 96 step rotation of the first wheel. Similarly the third wheel steps once for each rotation of the second, and so on through the eight wheels.

In a mechanical system, rotors are advanced mechanically and enciphering a character means following that character's pathway from the first rotor wheel through a series of permuted alphabet rotor wheels and out of the last wheel. In the software rotor system, wheels are advanced by shifting the contents of a rotor wheel's memory array. Enciphering consists of taking a plain character to be an index position of the first wheel array. The contents of that position are used as an index to the second wheel, and so on until the cipher character emerges from the eighth wheel array.

An important speed and simplicity advantage is achieved by creating in advance a complete set of eight decoding wheels. These are the respective inversely permuted enciphering wheels, arranged in reverse with respect to the enciphering wheels. Encoding and decoding are now identical programs, the only difference being which set of wheels is used. Listing 1 illustrates the simplicity of ROTERM's basic algorithm using the 6502's "(indirect), indexed" addressing mode. The encoding wheels are created by eight user-specified seeds to a random number generator. These eight seeds constitute the key. Permutations driven by a random number generator are very easy to implement. The decoding wheels are then produced from the encoding wheels by the program. Figure 2 shows the layout of the wheel arrays in memory. Figure 3 illustrates a rotor wheel and its inverse decoding wheel.

LISTING 1. Illustration of Rotor Encryption Algorithm Using 6502 Code

```
        LDX  $08      X register = number of rotor wheels
        LDY  CHAR     Y register = character to be encrypted
ROTOR   LDA  (RA),Y   Load accumulator with Yth element of rotor wheel
                      whose base address is stored in RA and RA+1 (two
                      locations on page zero of memory)
        TAY           Transfer result to Y register to use as index of
                      next rotor wheel
        CLC           Clear carry bit in preparation for addition
        LDA  RA
        ADC  $80      Add $80 to address in RA and RA+1 (generate base
        STA  RA       address of next rotor wheel)
        LDA  RA+1
        ADC  $00
        STA  RA+1
        DEX           Decrement X register
        BNE  ROTOR    If X register greater than zero, do it again using
                      next rotor wheel
                      Otherwise finish with substituted CHAR in Y
                      register
```

Table 1

ROTERM MEMORY MAP

All addresses are hexadecimal

1500 - 152B	Code for Terminal Control
152D - 15FF	Display Routine
1600 - 16C3	Read Keyboard Routine
16C4 - 16D9	Read ACIA Routine
1700 - 170F	Control of CIPHER variable
1710 - 171B	Filters out ASCII control codes
171C - 177F	Encode/Decode and Rotate Wheels
1780 - 17B0	Rotate one rotor wheel pair subroutine
17B1 - 17CC	Generate address of next rotor wheel pair for Rotate subroutine
17D0 - 17D7	Rotor position indices
17DB - 17D8	Terminal and Control variables
1820 - 187F	Rotor Wheel 8 Inverse
18A0 - 18FF	Rotor Wheel 7 Inverse
1920 - 197F	Rotor Wheel 6 Inverse
19A0 - 19FF	Rotor Wheel 5 Inverse
1A20 - 1A7F	Rotor Wheel 4 Inverse
1AA0 - 1AFF	Rotor Wheel 3 Inverse
1B20 - 1B7F	Rotor Wheel 2 Inverse
1BA0 - 1BFF	Rotor Wheel 1 Inverse
1C20 - 1C7F	Rotor Wheel 1
1CA0 - 1CFF	Rotor Wheel 2
1D20 - 1D7F	Rotor Wheel 3
1DA0 - 1DFF	Rotor Wheel 4
1E20 - 1E7F	Rotor Wheel 5
1EA0 - 1EFF	Rotor Wheel 6
1F20 - 1F7F	Rotor Wheel 7
1FA0 - 1FFF	Rotor Wheel 8

The Programs

ROTERM consists of two main parts, a BASIC program and a group of machine code routines. The BASIC program is the user interface for entering keys, terminal parameters, etc. This program consists of a menu of functions. Upon running the BASIC program, the user is presented with the following menu:

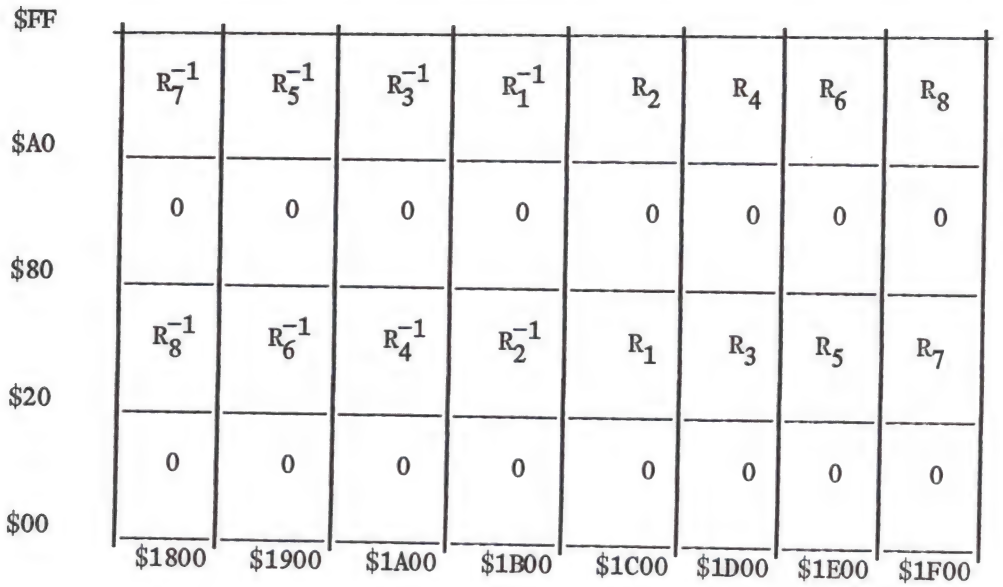


Figure 2. Chart of rotor wheel arrays in memory.

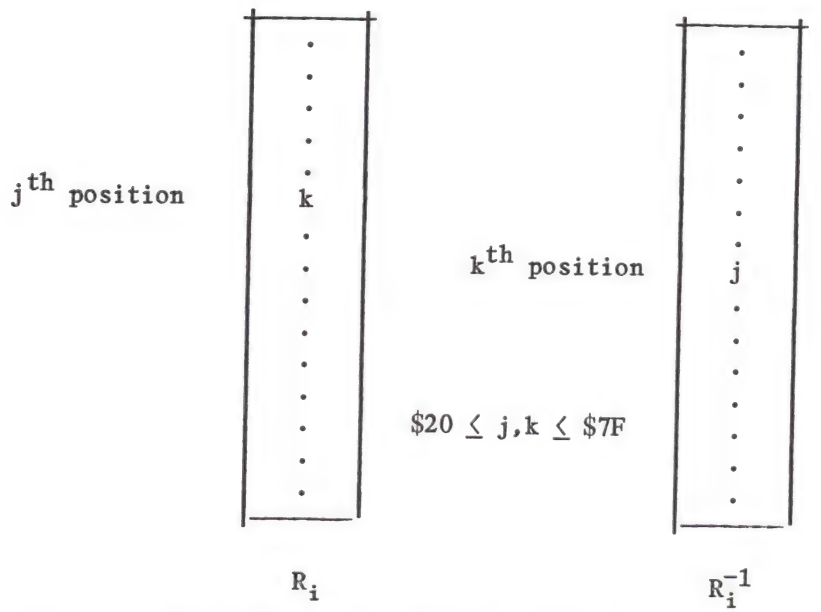


Figure 3. Rotor wheel pair showing inverse relationship of permutations.

KEY	ITERATE
LINE	PRE-SET
DUPLEX	START
MODE	TAPE

CHOICE?

Each of these menu options controls a specific action of ROTERM. The user need only type the first letter of the action he wishes to execute, followed by a carriage return (CR). The actions perform the following functions:

KEY - The user is asked to enter a 16 digit (decimal) key. The key wheels are generated along with their respective inverses, and all wheel position indexes are set to zero. The 16 digit key is broken up into eight 2-digit keys for the individual code wheels.

LINE - The user may enter a choice of terminal line lengths up to 24 characters.

DUPLEX - Asks the user if half duplex is desired. A Y(ES) response sets half duplex. Full duplex is set on any other response to this prompt.

MODE - Asks the user to choose one of three options for controlling the enciphering/deciphering process. ENCODE sets MODE equal to zero and activates possible encipherment of keyboard characters only. DECODE sets MODE equal to one and restricts possible decipherment to incoming (ACIA, serial port) characters only.

BOTH sets MODE equal to two and allows both encipherment of keyboard characters and decipherment of incoming characters.

Ultimate encipherment and decipherment of all characters is controlled by the value of another variable called CIPHER (see below).

ITERATE - To provide additional security to ROTERM, the user may choose some arbitrary number of dummy iterations of the cipher wheels. The wheels and their position indexes are advanced by the number of iterations chosen.

PRE-SET - Each wheel's index value (0 to 95) may be independently set. This offers even more security since it allows an arbitrary number of steps of wheel N to cause a step of wheel N+1, rather than the usual 96 step control.

START - Causes entry into the machine code endless loop terminal program.

TAPE - Executes a dump of the BASIC program to tape.

All functions except START and TAPE return to the menu after completion. This permits independent control of key and terminal parameters by the user.

The machine code program functional flow is best illustrated by the accompanying flow chart in Figure 4. The cipher system is thus embedded in a "smart" terminal program. The CTRL-Z and CTRL-V are this terminal's "smarts." They are recognized as control codes to switch the system between CLEAR and CODE operation. ASCII control characters (0 to 31 decimal, including line feed, carriage return, etc.) are untouched by the cipher process. This results in a great user convenience. Even in CODE operation, users can send one another normal control characters. This is very handy when using the terminal with a time sharing computer network or electronic mail network. The CTRL-Z and CTRL-V characters are in this class.

CONTROL

From the flowchart it can be seen that four variables govern the behavior of ROTERM:

1. I/O 0 = KEYBOARD, 1 = SERIAL PORT (ACIA)

2. MODE 0 = ENCODE, 1 = DECODE, 2 = BOTH

3. CIPHER 0 = CTRL-V, 1 = CTRL-Z

4. DUPLEX 0 = FULL, 1 = HALF

MODE is the master variable, and is fully controlled by the user. It is the user choice of restriction of possible encoding and decoding to incoming or outgoing characters or both.

I/O denotes the origin of a character to be processed. It is generated entirely by the program.

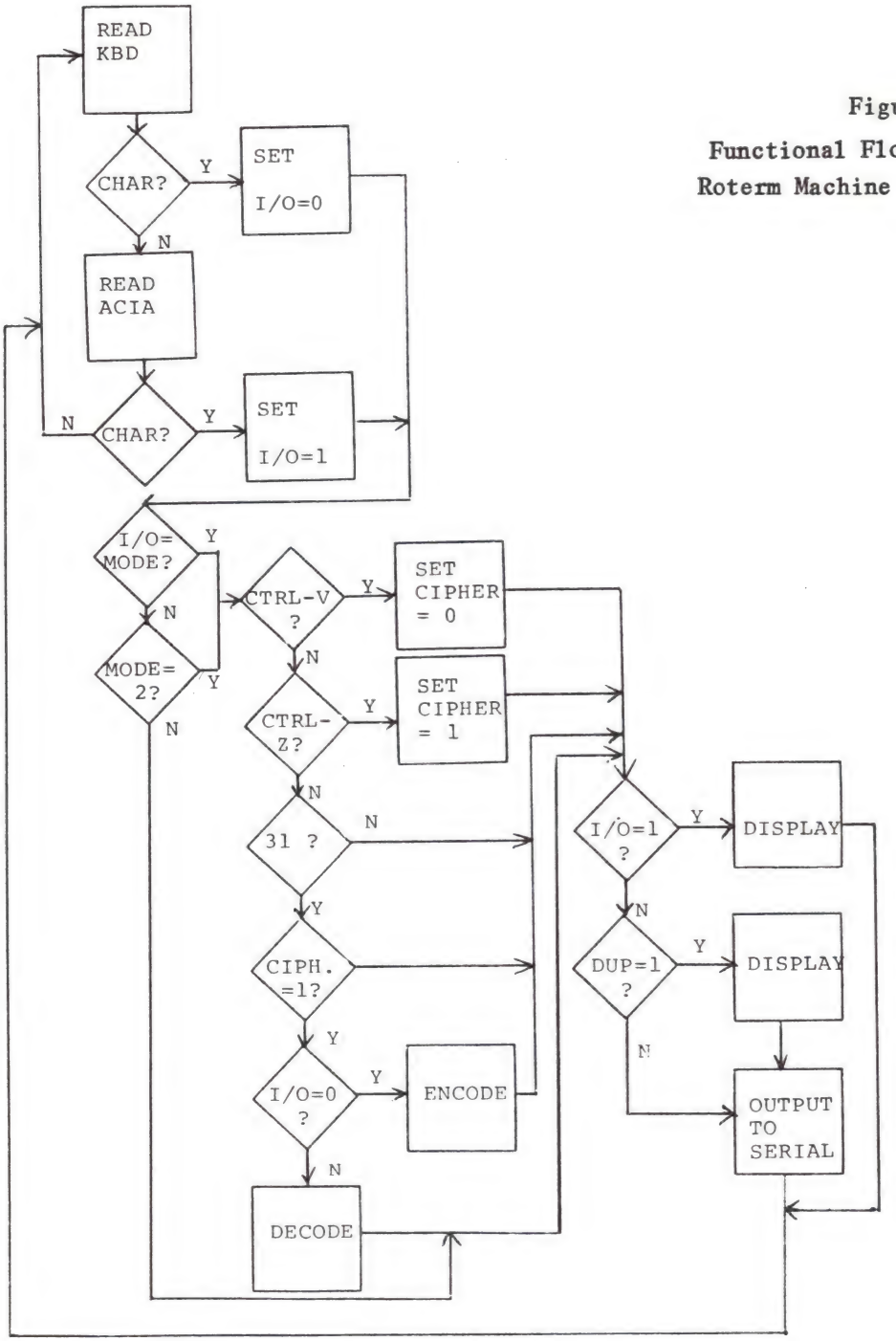


Figure 4
Functional Flow of Roterm Machine Code.

Table 2. Behavior of ROTERM modes.

MODE	ENCODE (0)	DECODE (1)	BOTH (2)
Entry to CIPHER mode (SET CIPHER = 1)	CTRL-Z on keyboard	CTRL-Z from serial port	CTRL-Z from keyboard or serial port
Entry to CLEAR mode (SET CIPHER = 0)	CTRL-V on keyboard	CTRL-V from serial port	CTRL-V from keyboard or serial port
Encryption (IF CIPHER = 1)	Outgoing characters (keyboard)	none	Outgoing characters (keyboard)
Decryption (IF CIPHER = 1)	none	Incoming characters (serial port)	Incoming characters (serial port)
Full duplex (DUPLEX = 0)	No display of outgoing chars. Expects echo from host, which is then displayed	No display of outgoing chars. Echoed chars. are decoded then displayed	No display of outgoing chars. Echoed chars. are decoded then displayed
Half duplex (DUPLEX = 1)	Displays all outgoing and incoming chars. No echo expected	Displays all outgoing and incoming chars. No echo expected	Displays all outgoing and incoming chars. No echo expected
Wheel rotation	One step for each encoded outgoing character, none for incoming ones	One step for each decoded incoming character, none for incoming ones	One step for each outgoing or incoming character.

CIPHER is controlled by the appearance of CTRL-Z and CTRL-V from the keyboard (if MODE equals 0 or 2), serial port (if MODE equals 1 or 2). Only if CIPHER equals 1 can any character be processed through the cipher wheels.

These four variables have 24 possible combinations. Table 2 shows how ROTERM behaves for sub-combinations of CIPHER, I/O, and DUPLEX. The overall master control function of MODE is also shown in this table.

In CLEAR operation (CIPHER = 0) all characters are processed in the clear, regardless of origin. CLEAR allows users to establish communication with a host or another user in simple English. It operates like a normal terminal. CODE operation (CIPHER = 1) allows enciphering and deciphering depending upon the values of the other variables.

Full duplex means that each character from the keyboard is sent out over the serial port without being displayed. The host correspondent system will echo the character back, whereupon it is displayed.

All incoming characters are always displayed. In half duplex operation, each character is displayed regardless of origin. The host does not echo received characters back to the terminal. The system can operate in either fashion as usage requires.

FUNCTIONAL OPERATION

There are three likely applications for ROTERM; user-user direct communication, single user posting of electronic mail, and single user reading of such posted messages.

User-user communication is best accomplished with MODE = 2 (BOTH) and half duplex (DUPLEX = 1). The ROTERM program will not behave like a commercial time sharing system, it has no provision to echo characters back to the sender. If full duplex is used, no outgoing characters will be displayed. The receiver's system won't echo, and the result will be no display at all on the sender's terminal. This might be useful in some circumstances. The half duplex assures display of outgoing characters. That MODE = 2 assures wheel synchronization of both parties. Both users can type in a CTRL-Z to place <u>both</u> terminals in CODE operation, or CTRL-V to resume CLEAR operation.

EXAMPLE:

Users "A" and "B" wish to communicate. Each starts ROTERM with the same key. They establish contact in CLEAR operation. Both users use half duplex and MODE = 2 (BOTH). "A" types a CTRL-Z to switch to CODE operation and starts sending encrypted characters to "B." "B" receives the CTRL-Z over her serial port which automatically switches her terminal into CODE operation to decrypt subsequent characters sent by "A." When "A" is finished, he types a CTRL-V to end his message to "B." This forces both terminals into CLEAR operation again. Even prior to the CTRL-V, "B" could transmit cipher characters to "A" while both are still in CODE operation. Wheel synchrony is carefully maintained. For each cipher character sent by "A," his rotor wheels advance one step. "B"'s rotor wheels advance one step for each character received and decoded. Both parties' rotor wheels are always in identical index positions. The users may communicate interactively, like a telephone conversation if desired. If either party becomes desynchronized, he or she may transmit a CTRL-V to force the other into CLEAR operation for a restart.

Posting electronic mail is best done using MODE = 0 and full or half duplex as necessary. ENCODE (MODE = 0) guarentees that (if full duplex is in use) echoed characters are not run through the rotor wheels. Only outgoing characters are enciphered; received characters bypass the rotors entirely.

EXAMPLE:

"A" wishes to post an encrypted message to "B."

"A" starts ROTERM, selects MODE = 0 (ENCODE) and full or half duplex as required. "A" establishes communication with the host computer in CLEAR operation. "A" types a CTRL-Z as the first character of the message. This converts his terminal to CODE operation. "A" types in the rest of the message and sees the resulting coded characters in his display. "A" closes the message with a CTRL-V, which brings his terminal back into CLEAR operation. "A" can now respond to host system prompts. "A" instructs the system to post the message to "B." Each encoded character sent by "A" advances his rotor wheels one step. Received characters bypass the rotors.

Receiving and decoding a posted message is best done with MODE = 1 (DECODE) and either full or half duplex. MODE = 1 forces all received characters to be decoded if CIPHER = 1. In this mode "B" cannot manually switch between CLEAR and CODE operation. The terminal passively awaits a CTRL-Z or CTRL-V over the serial input port to switch. Full or half duplex should be chosen appropriate to the host system. In this case, when the terminal is in CODE operation, each received character advances the rotor wheels one step while outgoing characters bypass the rotors.

EXAMPLE:

"B" wishes to read the encrypted message posted by "A" in the last example. "B" loads ROTERM with the same key as "A" used. She establishes communication with the host system in CLEAR operation. She has chosen MODE = 1 (DECODE). "B" requests to read the message. The first character is a CTRL-Z left by "A." This forces "B"'s terminal into CODE operation. Subsequent characters are decoded and displayed. The final character of the message is a CTRL-V. It resets "B"'s terminal into CLEAR operation for logoff, etc.

A great deal of care is devoted to correctly synchronizing "A"'s and "B"'s rotor wheels. The above examples have been tested by the author.

Because of the length of the program listings they are not printed here. The flowchart in Figure 4 presents the logical and functional structure of the machine language programs used in ROTERM. A complete listing of the disassembled machine code and BASIC program is available from the author for $1.00. A fully auto-loading cassette tape of ROTERM (for OSI C1P or Superboard II only) is also available from the author for $10.00.

CRYPTANALYSTS' CORNER

GREG MELLEN

William Friedman discovered and named the index of coincidence.[1] Kullback developed a statistical means of calculating it.[2] Kullback's equation calculates "kappa sub r," which is one means of expressing IC. The equation is:

$$k_r = \sum_{i=1}^{n} p_i^2 f_i \qquad (1)$$

where the f_i are the frequencies of the various characters in the set and the P_i are the probabilities of the characters. The reader will find, if he cares to work the equation, that the value for random text is .0385, and that for normal English approximately .0658 ("approximately" because the value will vary slightly depending on the standard frequency table used). Kullback discusses this on pages 81-85 et passim.

For the analysis of ciphertext, the delta IC is a more useful form of this equation:

$$\Delta IC = \Sigma(f_i(f_i-1))/(N(N-1)/i) \qquad (2)$$

where the f_i (used below) are from the frequency table on page 3 of Kullback's work and N is the number of characters in the message being analyzed. For the nonalgebrician, we'll calculate the ΔIC for standard English:

$$\Delta IC = ([A]\ 7189(7188) + [B]\ 1146(1145) + \ldots + [Z]\ 101(100)) / (100{,}000(99{,}999) / 26) = 1.71$$

More than two decimal places are useless, and fewer than two can mix the chaff with the wheat. Table 1 below continues what may seem to be an irrelevant essay. The table gives the standard deviation (σ) of ΔIC for standard English text for messages of various lengths.

Table 1.

N	σ	N	σ	N	σ	N	σ
15	.49	35	.20	55	.13	75	.09
20	.36	40	.18	60	.12	80	.09
25	.29	45	.16	65	.11	85	.08
30	.24	50	.14	70	.10	90	.08

Thus an English text 50 characters long will, two-thirds of the time, have a ΔIC of 1.72 ± .14. Obviously these calculations do not apply to manipulated text such as the harder Aristocrats in the Cryptogram. Though some creators may not realize it, the constructor of a hard simple substitution text is striving to make the ΔIC as low as possible (or, sometimes, as high as possible by repeating the same letter as frequently as he can).

When measuring the ΔIC of a ciphertext, you must use for comparison the "base ΔIC" yielded by the appropriate frequency table, whether for military test or for literary text. Depending on the frequency table used, the base may vary from about 1.67 to about 1.72. Other languages have different bases.

This background is completely unnecessary for readers who solved the short problem in the last column. Those who tried and were unsuccessful may now succeed if the need arises again.

The last problem was given as being in a progressive system using the EXTRICABLY sequence below as at least one of its components:

E X T R I C A B L Y D F G H J K M N O P Q S U V W Z

Had this sequence been both primary and secondary, the sequence or one of its 25 decimations would have solved the problem by decipherment at a period of 26. At this period, frequency data would be useless because there were only 104 characters, giving a depth of four to the frequency count. Even if each of the 26 decimations had been used to decipher the text, none would have yielded obvious plaintext for a reason which will emerge shortly.

But suppose a <u>total</u> frequency count is made on the incoherent text from each trial decimation. When the first 26 letters of the message, sufficient to calculate ΔIC with a tolerance of ± .28, are completed along decimation interval + 25 of the EXTRICABLY sequence, the following result is obtained:

ct : P H K K V W D G J R O I W E E L T U R C Z U C Z D O
pt?: P J N O X R M P U G T K D H J V O H Q W P N X U L N

Using equation (2), the ΔIC is computed and found to be 0.95, less than expected for random. The test is repeated at decimation interval +1:

```
ct  : P H K K V W D G J R O I W E E L T U R C Z U C Z D O
pt? : P G H G P P I C A Q L P G H G P G C F G C X Y T G P
```

The distribution now works out to the startling ΔIC of 3.47. Statistical buffs will see that this is a whopping 8.5 standard errors away from random, but such are the vagaries of English. If the converted text does not represent plaintext at least a statistical record has been set.

When the entire message is transcribed at the +1 decimation, the favorable results are sustained, and the message has been converted to monoalphabetic form. When it is solved by simple substitution, the message is found to begin: REFERRING TO REFERENCE NUMBER . . .

In carrying out this procedure, it is immaterial where the starting point is because the monoalphabetic text from the second level and from all other levels is isomorphic with the first level.

To recover the original primary component, the mechanics of encipherment may be invoked. At the start of encipherment, R_p was over P_c;

```
- - - - - - - - - - - - - - - - - - - - - R - - - - - -
E X T R I C A B L Y D F G H J K M N O P Q S U V W Z
```

The secondary component was then shifted one place to the right to encipher the second plaintext letter, so that R_p was over Q_c and E_p was over H_c:

```
- - - - - - - - - - - - - - E - - - - - - R - - - - -
E X T R I C A B L Y D F G H J K M N O P Q S U V W Z
```

The reconstruction is continued for the first 25 letters of the message, at which point the encipherment device appears thus:

```
U B - I N G - - - - C E F - - - - - R T - - - - - -
E X T R I C A B L Y D F G H J K M N O P Q S U V W Z
```

Those who persist in the solution will find that the primary sequence is based on the keyword SUBKINGDOM.

This technique does not exhaust the possibilities for solving progressive systems. For example, when a number of short messages are in hand which use the same primary and secondary components, they may be written at a period of

26 and placed in depth by using repetitions in the ciphertext. One message may be slid along another, or a group of messages already in depth, until the offset which yields the highest ΔIC is found.

For the next set of problems, the reader is on his own until January, when some help will be given. Given the methods discussed here over the past year, the reader may be assured that at least some of them apply. A device developed in a European country, apparently around the time of World War I, was used to encipher the problems, which are nevertheless in English.

(1)
VV3B4 BTYZ3 JNRGM W3FAQ NQWGG KDMI3 HXJTL 3IOWJ EM4L4 2FKRQ
GCNMT KNGV3 KTEZE UDAS4 SYJRS 2LBIM MCCNM LTNNR JTDO3 QNEYZ
ILYHM AFKIP AJCUB VGBWK RVNIO VVD43 EEA3M LTAIA

(2)
KKWDF WNOTR WOUDX QWEYL 4LF4T JNUEV CQY3D YTWVS 3DWHL 2EFK2
4CHJ3 MQHJP LFBIV XNYHJ VBDX2 URLAC DF2MH 4PNYV FMBOI NRNKE
2GVZY EHZIX Z4SEH 44MJH BMKGQ MTGRC

(3)
22EDJ DOFBA RBQQU WIERV NZPUB 3L2H2 ETCZM FKIPA JIUIO 2GWRX
ZXHAZ 3DWXA ZCSMJ 3SIIX IKHKG QUTWQ STB3W XMSYJ WMF4N NMIUQ
4QIZT YMS3B F4DTY 32MLK KPC2A FKNFK QENUU 20XRF XISAL PDCK4
PR43Z GBVVR GZXEB BOPBZ 2HC3C LOFSE JXKEU RZREB CX4H3 EPA23
DAQAN WKTLM 4GKQY BYX4U SFXEG TYEC2 MRPFL GPCNM QAUMK RUX3E
RZGXU U3MVP EPRZZ D3RHG PNMA2 ORBJR GOUWS AZ3DW FHESZ G3PDP
MIFPK JHQKK GQLRR SQBEV UZEEF ZY4F2 MV3UJ QAPIQ QY3BO XROZ3
PI2GD

(4)
KKR42 CAEZA YQCYX OV43W HF2EJ EBQLN NCVQI YFHYG HDXDZ PE3PJ
4PSFO DZVKI JZTLI OKOWR YIZIM UVYDC LKHTY E3JCJ TKKPX HAYSG
DMFYA NTDBH ZFZWE PLJK4 CHMPC KRYPM BVBQX 3OZOU DLOWF IAHH4
4CHFM CCLDM XNYJC BUVAF USH3E PA23D 4QIRK ITPLR CANRR XZYBB
3YHFM 3A3RF LTJTG CUVQR ITGWS TB2ML WJJD4 HCR4J UIMA4 P3KRV
NIOVV NKPLL CS4DQ 4CHDJ JBHKY WGESG

REFERENCES

1. Friedman, W. F. The Index of Coincidence and Its Applications in Cryptography. Publication No. 22, Riverbank Laboratories, Geneva, IL., 1922. (Reprinted Laguna Hills, CA: The Aegean Park Press, 1979.)

2. Kullback, S. Statistical Methods in Cryptanalysis. Washington, DC: U.S. Government Printing Office, 1935; Revised 1938. (Reprinted Laguna Hills, CA: The Aegean Park Press, 1976.) The frequencies in equation (2) are from Figure 1, page 3.

BOOK REVIEWS

LOUIS KRUH

BIBLIOGRAPHY OF INTELLIGENCE LITERATURE

Cline, M.W., E.E. Christiansen, and J.M. Fontaine, eds. Scholar's Guide to Intelligence Literature: Bibliography of the Russell J. Bowen Collection. University Publications of America, Inc., 44 N. Market St., Frederick MD 21701. 1982. 236 pp. $40.00.

This is a big book and an important work prepared under the auspices of the National Intelligence Study Center. It is based on the Bowen Collection of intelligence literature now deposited at the Lauinger Memorial Library at Georgetown University. The bibliography covers more than 5,000 titles and its scope is indicated by the 372 headings and subheadings, which include National Intelligence Establishments, Clandestine Operations, Espionage, Reconnaissance, Codes and Ciphers, Research and Analysis, Counterintelligence, Warfare, Covert Action, Intelligence Support, Unconventional Warfare, and much, much more. Besides the section on codes and ciphers, works which include references to cryptology may be found under many other headings. This first, book-length, bibliography on intelligence is a most comprehensive checklist which will be a valuable reference guide for further study for anyone interested in any aspect of the intelligence service.

MILITARY COMMUNICATIONS - JANE'S BOOK

Raggett, R.J., ed. Jane's Military Communications 1983, 286 Congress St., Boston MA 02210. 1982. 839 pp. $140.00.

This is a big book, 9" X 13", weighing at least five pounds, printed on heavy quality paper by the publishers of the famous Jane's Yearbooks. There are chapters on Radio Communications, Line Communications, Data Transmission, Message Switching, Electronic Warfare, Facsimile, Laser and Optical, Encryption and Security, and others. Each section is divided by country and contains a complete description of the equipment involved, usually with photographs and specifications. In the encryption section the countries

represented are Austria, Belgium, France, Germany, Israel, Italy, Spain, Sweden, Switzerland, United Kingdom and USA. Some of the crypto equipment described includes Off line Telex cipher units, key generators, cipher machines, scramblers, tactical digital ciphering equipment, pocket cipher units, portable secure message terminals, burst message transfer sets, digital bulk ciphering devices, teleprinter ciphering units, narrow-band privacy equipment plus much, much more. A chapter on Major Systems describes the overall military communications systems of various countries and NATO. For the US, it includes the World-Wide Military Command Control System, Tri-Tac Joint Tactical Communication System and many others. Appendices include acronyms and code names, numbered communications equipment and a directory of manufacturers. As with other Jane's Yearbooks, this hugh volume is a veritable warehouse of information (even the advertisements are informative) and a guide to the state of the art in cryptographic equipment available for military use today.

NAVY RADIO INTELLIGENCE ACTIVITIES MEMOIRS

Lewis, G.A., ed. Intercept Station "C" From Olongapo Through the Evacuation of Corregidor, 1929-1942. Naval Cryptologic Veterans Association, 3065 Olive St., Denver CO 80207. 1983, 83 pp. $9.00.

This is the story, mostly human interest, of the pre-WW II U.S. Navy Radio Intelligence Activities in the Philippine Islands and the evacuation of USN Communications Intelligence personnel from Corregidor. It is a series of short personal narratives by individuals who were there plus material taken from recently declassified publications. A fascinating history with many photographs and diagrams.

FRENCH RESISTANCE - NEW TRANSLATION

Lorain, P. Clandestine Operations. Macmillan Pub. Co., 866 3rd Ave., New York NY 10022. 1983. 185 pp. $24.95.

Published originally in French, this excellently illustrated English adaptation by David Kahn, describes the weapons and techniques used by the French Resistance, 1941-1944.

The author, an amateur radio operator, antique weapons expert and architect, tells how the Free French worked with British military intelligence. He describes in words and drawings their weapons; ingenious containers for explosives and radio equipment; various planes used to deliver equipment and

messages; revolvers and machine guns; and pistol pens and knives which were standard gear for Resistance fighters. He recounts the procedures taken to elude detection while sending and receiving radio messages. The radio sets are pictured and he relates the direction-finding techniques used by the Germans to locate clandestine stations.

An extensive chapter is devoted to the codes and ciphers used by the Resistance including the Playfair, Double Transposition, A-Z System, Delastelle, One-Time Pad, superenciphered codes, and others. Examples and illustrations are provided to insure understanding. It is an unusual book on an unusual subject with information and drawings unavailable elsewhere.

MYSTERY NOVEL CIPHER

Eco, U. The Name of the Rose. Harcourt, Brace, Jovanovich, 1250 Sixth Ave., San Diego CA 92101. 1982. 502 pp. $15.95.

This tale of a murder investigation in a monastery in the 14th century includes a great deal of scholarly information on heretical movements, monastic orders, and the daily life of monks. The author, a professor of semiotics, includes obscure clues, mysterious ciphers, and a library with secret rooms in his entertaining work, which has been a best seller in Europe and widely acclaimed in this country.

OLD CLASSIC CRYPTOGRAMS DISCOVERED

Ohaver, M.E. Solving Cipher Secrets, A Collection of Weekly Articles from Flynn's Weekly Detective Fiction, 1927-1928. Aegean Park Press, Box 2837, Laguna Hills CA 92653. 1982. 153 pp. $18.80.

This book is a compilation of the first 73 weekly columns written by Ohaver, starting in 1927. These columns provide a fascinating and excellent collection of cryptologic information. Each column contains ciphers for readers to solve and in succeeding columns the author explains the techniques for solving them. A great variety of systems are covered in this manner with the more difficult ciphers, e.g., double transpositions, featured in several columns. Ohaver wrote about historical ciphers, price mark ciphers and many unusual and interesting cryptograms. It is amazing to see how well and extensive the subject of cryptology was written about more than a half century ago.

OSS FOUNDATION FOR CIA - AN ACCOUNT

Smith, B. A. The Shadow Warriors: OSS and the Origins of the CIA. Basic Books, Inc., 10 E. 53 St., New York NY 10022. 1983. 507 pp. $20.75.

This is a comprehensive account of the beginnings of the nation's first centralized intelligence agency, how it was created and operated, what it really accomplished and how it laid the foundation for the present CIA. The complex and fascinating story includes references to Ultra and Magic decrypts but points out they were withheld from the OSS. Stories of secret missions are numerous but one of the most surprising is about the OSS purchasing information on Russian codes from Finnish sources in 1944 contrary to advice from the State Department and then giving the material to the Russians.

THE STATE OF THE ART CONFERENCE IN CRYPTOLOGY - CRYPTO 82

Chaum, D. , R. L. Rivest and A. T. Sherman, eds. Advances in Cryptology: Proceedings of CRYPTO 82. Plenum Pub. Corp., 233 Spring St., New York NY 10013. 1983. 331 pp. $45.00.

CRYPTO 82, a workshop on the theory and application of cryptographic techniques, held at the University of California, Santa Barbara, in August 1982, attracted over 100 participants, including many of the world's leading researchers in cryptology. This official record of the conference contains 34 papers that were presented plus a paper from CRYPTO 81 which did not appear in the 1981 proceedings. The papers provide a look at the current unclassified state of the art cryptologic research being conducted at universities, laboratories and corporations. Familiarity with some advanced mathematical concepts is needed for a full understanding of the presentations. The book, like the conference, is arranged in six sections: (1) Algorithms and Theory, (2) Modes of Operations, (3) Protocols and Transaction Security, (4) Applications, (5) Special Session on Cryptanalysis, and (6) Rump Session: Impromptu Talks by Conference Attendees. The meeting created national news with separate presentations by Adi Shamir and Leonard Adleman which explained how to break some knapsack ciphers previously thought unbreakable. This book is must reading for the serious student of cryptology and the exposition is excellent.

BIOGRAPHIES OF CONTRIBUTORS

Greg Mellen is a staff engineer in the Sperry Univac Civilian Agency Systems Engineering Department. His interest in ciphers and language date back to his training as a classicist and his work as a cryptanalyst. Address: 8441 Morris Circle, Bloomington MN 55437.

Louis Kruh is a public relations executive with the Bell System in New York City. His interests in cryptology span more than forty years. He collects crypto material and machines. He has a BBA, cum laude, from the City College of New York, and an MBA, with distinction from Pace University. Currently he is nearing completion of law school. Address: 17 Alfred Road West, Merrick NY 11566.

Peter Winkler is an Assistant Professor of Mathematics and Computer Science at Emory University. He holds a BA from Harvard University (summa cum laude) and a PhD in mathematics from Yale University. He is a former cryptologic officer. Address: Department of Mathematics and Computer Science, Emory University, Atlanta GA 30322.

Daniel Wolf is a marketing specialist for a manufacturer of CAT scanners and other computer-based radiologic equipment. He has a BS in Physics and an MS and PhD in Zoology, all from the University of Illinois. He spends his spare time writing for computer user-group journals on communications techniques and playing Dobro guitar. Address: P O BOX 565, Port Hueneme CA 93041.

Albert C. Leighton is Professor of Ancient and Medieval History at the State University of New York College at Oswego. After twenty year's enlisted and commissioned service in the United States Army Security Service he retired and earned his AB, MA, and PhD from the University of California at Berkeley. he has written on diverse subjects, "Transport and Communication in Early Medieval Europe," "The Horse and Human History," and "The Mule as a Cultural Invention," in addition to many works on cryptology. In 1978-79 he was a Fulbright Research Professor at the University of Munich. REcently he was named Faculty Research Scholar for the entire SUNY system with such subjects in his repertoire as "Medieval Mules - A Study in Asinine Sexual Behavior," and "The Love Life of Millard Fillmore." Address: Department of History, State University of New York College at Oswego, Oswego NY 13126.

Stephen M. Matyas is a member of the Cryptography Competency Center at IBM's development laboratory in Kingston NY. Dr. Matyas holds several patents and has published numerous technical articles covering all areas of cryptographic system design. He is coauthor of the recent book, Cryptography - A New Dimension in Computer Data Security, and is a contributing author to Encyclopedia of Science and Technology and Telecommunications in the US: Trends and Policies. He received his PhD in computer science from the University of Iowa, writing his thesIS on a subject of cryptanalysis. Address: IBM, Building 001 Neighborhood Rd., Kingston NY 12401.

Oskar E. Stuerzinger received the Swiss Baccalaureate C in 1940. During the war he studied at the Swiss Federal Institute of Technology, while serving in the Swiss Signal Corps. He joined a local R and D factory which had developed a small field teleprinter for the Swiss Defence Forces. There he met Boris C.W. Hagelin from Stockholm, Sweden. The idea to develop a cipher teleprinter was in the air. In 1952 Hagelin decided to have his own laboratory in Zug, Switzerland. Stuerzinger was hired as the first and then only employee of the newly founded CRYPTO AG. Soon the company was producing fine mechanics and technicians. In 1958 the activity in Stockholm was closed and in 1966 CRYPTO AG moved to a new site in a suburb of Zug. Mr. Stuerzinger retired as Technical Director from CRYPTO AG in 1980. Address: Kirchmattweg 6, CH-6340 Baar (ZG), Switzerland.

Hugo Brändström received the BSc degree from the University of Stockholm in 1951. He received degree liceantiate of technology in 1968 and the doctor's degree in 1978 from the Royal Institute of Technology, Stockholm. From 1952 to 1963 he was employed at the Research Institute of National Defense. In 1963 he worked at the Axel Johnson Institute for Industrial Research and then in 1964 he moved to AB Teleplan, Solna Sweden. His main interests are in algebraic systems with applications. Address: AB Teleplan, P O BOX 1310, S-17 1 25 Solna Sweden

INDEX TO CRYPTOLOGIA, VOLUME 7 (1983)

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal with issue dates of January, April, July and October. The four journals issued each year constitute one volume. The January 1983 issue is Volume 7, Number 1.

Subscription prices (U.S. Dollars): $28.00 per year for U.S., $36.00 per year for non-U.S. Air Mail overseas rate is $60.00 per year. A subscription begins with the current issue as of date of receipt of request unless otherwise instructed. Back issues from January 1979, Volume 3, Number 1 to current issue are available from the Editorial Offices for $8.00 each in the U.S. and $10.00 each to non-U.S. address. Specify volume, number and issue date.

All orders, checks and inquiries should be sent to: CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803, USA. Make checks payable to CRYPTOLOGIA.

Note to subscribers: The number in the upper right corner of your address label indicates the last issue of your subscription. The right hand (single) digit indicates the Number and the remaining left hand digit(s) indicate the Volume of the last issue in your subscription. Renew your subscription now.

CALL FOR PAPERS

CRYPTOLOGIA welcomes articles on all aspects of cryptology. We especially seek articles concerning mathematics and computer related aspects of cryptology. Articles describing new cryptosystems and methods of cryptanalysis of cryptosystems, historical articles, memoirs and translations are all sought.

Send mathematical and computer related papers to Brian J. Winkel, Division of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Send papers, inquiries and letters concerning cryptographic machines, devices and equipment to Louis Kruh, 17 Alfred Road West, Merrick, NY 11566.

Send historical and other nontechnical articles to David Kahn, 120 Wooleys Lane, Great Neck, NY 11023.

Any paper may also be sent to the Editorial Office, CRYPTOLOGIA, Rose-Hulman Institute of Technology, Terre Haute, Indiana 47803.

Three copies should be submitted and one should be kept by the author as a protection against loss. Manuscripts should be legibly typewritten, or reproduced from typewritten copy and double-spaced with wide margins. All papers should have an Abstract and a Key-Word List after the title and author. Editorial style follows the University of Chicago Press Manual of Style. Please adhere to the footnoting style found in CRYPTOLOGIA articles. Diagrams should be done in black, suitable for off-set photo reproduction, and clearly labeled with a legend. Photographs should be clear and glossy. Indicate whether or not the photo print enclosed is to be returned.

While the ultimate responsibility for the accuracy of the material presented lies with the author(s), the Editorial Office will do its best through the refereeing and consultation process, to help insure correctness.

Authors will receive two copies of the issue in which their articles appear.

CRYPTOLOGIA

A Quarterly Journal Devoted to All Aspects of Cryptology

Volume 7 Number 4 October 1983

Table of Contents

Published Quarterly at

Rose-Hulman Institute of Technology

Terre Haute, Indiana 47803 USA

(Vol. 5 cont.) Number 4

The Genesis of the Jefferson/Bazeries Cipher Devices
A User's Guide in Voice and Data Communications Protection -- Book Review
Letters to the Editor
Applications of the Drazin Inverse to the Hill Cryptographic System IV
Secret Writing Exhibit
Higher-Order Homophonic Ciphers
Number Theory in Digital Signal Processing--A Book Review
Interactive Solution of Columnar Transposition Ciphers

VOLUME 6 1982

Number 1

Mathematical Solution of the Enigma Cipher
In Memoriam: Marian Rejewski
Why Germany Lost the Code War
Enigma Solved
The Black Chamber
Wilderness of Mirrors--A Book Review
Beale Society Material--A Book Review
If I Remember
Cryptanalysts' Corner
Churchill Pleads for the Intercepts
A Conversation with Marian Rejewski
Unraveling the Enigma Story--A Book Review
From the Depths to the Heights--Book Reviews
Remarks on Appendix 1 to British Intelligence in the Second World War
Computer Cryptography -- Book Review
The Navy Cipher Box Mark II

Number 2

Use of Microcomputer System for Medical Record Encryption and Decryption Using a Sequential Pseudo-Random Key
The Performance of Hellman's Time Trade-Off against Rotor Ciphers
A New Source for Historians: Yardley's Seized Manuscripts
In Memoriam: Georges-Jean Painvin
Error-Correcting Codes and Cryptography--Part I
Cryptanalysts' Corner
Konheim's Cryptography--A Primer--A Book Review
Sirius

Number 3

Rhapsody in Purple, a New History of Pearl Harbor--Part I
Factoring Via Superencryption
The Mystery of Colonel Decius Wadsworth's Cipher Device
Cryptanalysts' Corner
Cryptographic Features of the UNIX Operating System
Error-Correcting Codes and Cryptography--Part II
Ciphertext Only Attack on the Merkel-Hellman Public-Key System under Broadcast Situations
Solution to Sirius Music Cipher
Helmich and the KL-7

Number 4

The Siemens and Halske T52e Cipher Machine
Cryptanalysts' Corner
Applications of Vincent's Theorem in Cryptography
Breaking a Pseudo Random Number Based Cryptographic Algorithm
Digital Signature Schemes
A Pedagogical Cipher
Rhapsody in Purple, A New History of Pearl Harbor--Part II
A Child's Garden of Cryptography
A Basic Probe of the Beale Cipher as a Bamboozlement

VOLUME 7 1983

Number 1

The Crypto '82 Conference, Santa Barbara A Report on a Conference
Cryptanalysts' Corner
Annotated Bibliography in Conventional and Public Key Cryptography
Fraternal Cryptography: Cryptographic Practices of American Fraternal Organizations
Language Redundancy and the Unicity Point
Cryptographic Protection of Files in an Automated Office
Application of a Certain Class of Infinite Matrices to the Hill Cryptographic System
The Power of Magic: A Book Review
Cipher Equipment: The Cryptographic Unit CSI-10
Uncaging the Hagelin Cryptograph

Number 2

A Failure of Radio Intelligence: An Episode in the Battle of the Coral Sea
Account of Gen. George C. Marshall's Request of Gov. Thomas E. Dewey
Abwehr Ciphers in Latin America
The Typex Cryptograph
Cryptanalysts' Corner
The Problem of Reciprocity in a Delastelle Digraphic Substitution
A "Weak" Privacy Protocol Using the RSA Crypto Algorithm
Remarks on a Digital Signature Scheme
The View from Across the Pond
The Noblest Cryptologist - Duke August

(Vol. 7 cont.) Number 3

An Unsolved Puzzle Solved
The Early Models of the Seimans and Halske T52 Cipher Machine
Eurocrypt 83: A Conference Report
DES-Generated Checksums for Electronic Signatures
Cryptanalysts' Corner
Book, Movie, Article and Game Reviews

Number 4

How to Use the German Enigma Cipher Machine: A Photographic Essay
The Search for the Key Book to Nicholas Trist's Book Ciphers
Examples of Intelligence Obtained from Cryptanalysis
The Advent of Cryptology in the Game of Bridge
The B-21 Cryptograph
A Public-Key Cryptosystem Based Upon Equations Over Finite Field
ROTERM: A Microprocessor Based Cipher Terminal System
Cryptanalysts' Corner

VOLUME 8 1984

Number 1

System for Verifying User Identity and Authorization at the Point-of Sale or Access
LUCIFER, A Cryptographic Algorithm
Reviews of Things Cryptologic
Who Did It?
Cryptanalyst's Column
Cipher Machine Inventor - Boris Hagelin Dies
Achievements of Cipher Bureau MI-8 During the First World War
Because of the Freedom of Information Act
The Mysterious Autocryptograph

Number 2

Cryptanalysis of a Maclaren-Marsaglia System
Project on Secrecy and Openness in Scientific and Technical Communication
Hand-Held Crypto Device SEC-36
Sidney Hole's Cryptographic Machine
Literature Reviews
Kullback's Chi-Tests for Matching and Non-Matching Multinomial Distributions
Software Protection for Microcomputers
Corrections for UNITED STATES CRYPTOGRAPHIC PATENTS: 1861 - 1981
The Slidex RT Code
British Intelligence - Volume II - Book Review
Codes and Ciphers for Combined Air-Amphibian Operations
An Unknown Cipher Disk

Number 3

The Origins of Russian Navy Intelligence
A Cryptographer's War Memories
Rear Admiral Joseph N. Wenger USN (Ret) and The Naval Cryptologic Museum
A View of Renaissance Cryptography - Review
Reflections on the "State of the Art"
Cryptology and the Law
Sir Percy Scott's Cipher
A Further Weakness in the Common Modulus Protocol for the RSA Cryptoalgorithm
The Resurrection of Multiple-Key Ciphers
AAAS Crypto Sessions Proceedings - Review
Cryptanalysts' Column
Cipher Equipment - TST 3336 and TST 9761
IACR Announces Bulletin Board Service

Number 4

The Heraldry Of Cryptology
Cryptography in Runic Inscriptions
Cryptanalysts' Corner
Cryptology and The Law
Alan Turing: The Enigma -- Book Review
Looking Back
A Generalization of the Knapsack Algorithm Using Galois Fields
Finding Vowels in Simple Substitution Ciphers by Computer
Cryptanalysis of Shift Stream Generated Stream Cipher Systems -- Book Review

CRYPTOLOGIA

CRYPTOLOGIA is a unique scholarly journal devoted to all aspects of cryptology. The journal began quarterly publication in 1977.

Areas covered include computer security, history, codes and ciphers, mathematics, military science, espionage, cipher devices, literature, and ancient languages.

Features include reviews of literature and equipment, news of the crypto community, announcements of activities, challenging ciphers, exchange column, and more.

CRYPTOLOGIA publishes a book on United States cryptographic patents. This is the definitive book listing and detailing over 2,000 cryptographic patents during the period 1861-1981. Richly illustrated, the work serves as a wealth of information for all cryptology enthusiasts. The book is by Dr. Jack Levine, Professor Emeritus of North Carolina State University.

ORDER BLANK FOR CRYPTOLOGIA ISSUES AND PATENT BOOK

Name _____

Address _____

_____

_____

[Volume 1, Nos. 1, 2, 3, 4, and Volume 2, Nos. 1, 2, 3, 4 are only available from University Microfilms, 300 North Zeeb Road, Ann Arbor MI 48106 USA.]

Volumes 3 - Current volume are available from CRYPTOLOGIA, Rose Hulman Institute of Technology, Terre Haute IN 47803 USA.

$8.00 each number - single and back issue price for US

$9.00 each number - single and back issue price for non-US

CHECK material desired, total and remit check in US dollars.

Vol.	III	IV	V	VI	VII	VIII
No.	1____	1____	1____	1____	1____	1____
	2____	2____	2____	2____	2____	2____
	3____	3____	3____	3____	3____	3____
	4____	4____	4____	4____	4____	4____

____ United States Cryptographic Patents, 1861-1981, by Dr. Jack Levine. $10.00. [With your one year subscription - $6.00.]

____ One or multiple (_____years) year subscription to CRYPTOLOGIA (begin with _____issue) Multiply years by rate. $28.00 (U.S.) $36.00 (non-US) $60.00 (non-US airmail) /yr.

** With two year subscription free Polish First Day Cover of stamp honoring Polish cryptanalysis of Enigma cipher.

*** With three year subscription receive Polish stamp cover and US Patent book.

Above offers valid while supply lasts.

AMOUNT ENCLOSED

____ number of back issues ordered $8.00(US) or $9.00(non-US) Total _____

US Cryptographic Patents, 1861-1981 _____

Subscription to CRYPTOLOGIA _____

Total Amount Enclosed _____

VOLUME 1 1977

Number 1

Why Cryptologia?
The Cryptology of Multiplex Systems--Part I
A Different Kind of Column
"Cracking" a Random Number Generator
The Biggest Bibliography--A Book Review
A Reply to Kahn's Review
Unicity Points in Cryptanalysis
Cipher Equipment
Some Cryptographic Applications of Permutation Polynomials
Poe Challenge Cipher Finally Broken

Number 2

Age of Decipherment
"Count Forward Three Score and Ten..."
Automated Analysis of Cryptograms
Cipher Equipment
The Cryptology of Multiplex Systems--Part II
Get Out Your Secret Decoders, Boys and Girls
Analysis of the Hebern Cryptograph Using Isomorphs
Rotor Algebra
Grille Reconstruction

Number 3

Significance of Codebreaking and Intelligence in Allied Strategy and Tactics
The Kappa Test
Word Ways, A Journal Worth Going Your Way
Entropy Calculations and Particular Methods of Cryptanalysis
Cipher Equipment
The Earliest Use of a Dot Cipher
DPEPE DPJO
Kullback's Statistical Methods in Cryptanalysis, A Book Review
Assessment of the NBS Proposed Federal Data Encryption Standard
Proposed Federal Information Processing Data Encryption Standard

Number 4

Ithaca Connection: Computer Cryptography in the Making, Special Status Report
Poe Challenge Cipher Solutions
A Rapid Yes-No Computer-Aided Communicator
MA4210 Alphanumeric Pocket Cipher
Ecclesiastical Cryptography, A Review
Equivalences of Vigenere Systems
Cryptography at the Colorado School of Mines
Cryptanalysis and Data Security Course at the University of Tennessee
Cryptanalytic Attack and Defense: Ciphertext-only, Known Plaintext, Chosen-plaintext
Reports form the Reich
The Churchyard Ciphers
CENSORED, A Simulation Exercise
German Military Eavesdroppers
The Enigma--Part I, Historical Perspectives
Preliminary Comments on the M.I.T. Public-Key Cryptosystem

VOLUME 2 1978

Number 1

Solving a Hagelin, Type CD-57, Cipher
Cryptanalysis Course Down Under
Forschungsamt: Nazi Germany's Most Secret Communications Intelligence Agency
Mathematical and Mechanical Methods in Cryptography
The Inventions of William F. Friedman
Remarks on Proposed Attack on MIT Public-Key Cryptosystem
Cryptanalysis of the Hagelin Cryptograph--A Book Review
Cryptanalyst's Corner
James Lovell and Secret Ciphers During the American Revolution

Number 2

Mathematical and Mechanical Methods in Cryptology--Part II
A Book Review--Friedman's Life, The Man Who Broke Purple
Cryptanalyst's Corner
Who Wrote The American Black Chamber?
Cryptology at Kean College
Nuggets from the Archives: Yardley Tries Again
The Unsolved D'Agapeyeff Cipher
Modern Methods for Computer Security and Privacy--A Book Review
Pictures Galore--A Book Review
Computer Methods for Decrypting Multiplex Ciphers
Casanova and the Beaufort Cipher
Cryptology as a Career
Encryption Challenge
DH-26 Handheld Encryption Unit
A Tribute to Alf Monge

(Vol. 2 cont.)

Number 3

My Recollections of G.2 A.6
Computer Methods for Decrypting Random Stream Ciphers
Cryptanalysis and Computers
Cryptanalysts' Corner
A Catalog of Historical Interest
Astle Cipher Solved
A Famous Variation--A Book Review
Reveling in Deception--A Book Review
Decoding Wesley's Diaries
Short Notices--Book Reviews
Hagelin Machine (M-209) Reconstruction of Internal Settings
Capsule Reviews for Crypto Buffs

Number 4

Security of Number Theoretic Public Key Cryptosystems Against Random Attack I
What the Nazis Were Doing
The Riverbank Publications on Cryptology
Extraordinary Codebreakers, Outstanding Family--A Book Review
A 19th Century Challenge Cipher
Cryptanalysis' Corner
A Catalog of Historical Interest--Part II
An Application of Computers to Cryptography
One of the Worst--A Book Review
Rent a Code
Action Line Challenge
Data Encryption Gurus

VOLUME 3 1979

Number 1

The Ultra Conference
How Did TJB Encode B2?
Report on the Decipherment of the American Strip Cipher 0-2
Courses in Cryptology
Security of Number Theoretic Public Key Cryptosystems Against Random Attack II
The HP-67/97 Cryptograph
A Xerograph of a Classic
Papers Disclose Allies' Edge in Knowing German Codes
A Sherlockian Cryptogram

Number 2

Early Work on Computers at Bletchley
The Hagelin Cryptographer, Type C-52
Solution of Challenge Cipher
American Codes--A Book Review
The Macbeth Test Message
Security of Number Theoretic Public Key Cryptosystems Against Random Attack III
A German Consular Cipher
Littlewood's Cipher
Ultra Goes to War--A Book Review

Number 3

NSA Perspective on Telecommunications Protection in the Nongovernmental Sector
J. F. Byrne and the Chaocipher - Work in Progress
Solving a Cipher Based on Multiple Random Number Streams
The Futility of It All
The Deadly Double Advertisement - Pearl Harbor Warning or Coincidence
Littlewood's Cipher: A Method of Solution The Two-Message Problem in Cipher Text Autokey I
How to Swindle Rabin

Number 4

Musical Cryptography
Cryptographic Aspects of Data Compression Codes
CP-III: One Time Cypher Pad Manual Encryption Device
The Geheimschreiber
Ciphers for the Educated Man
The Two-Message Problem in Cipher Text Autokey--Part II
A Musical Cipher
Language Redundancy and Cryptanalysis
The Day the Friedmans Had a Typo in Their Photo
Cryptanalysis' Corner
A German Code Book
A Theory of Cryptography

VOLUME 4 1980

Number 1

The Solution of a Cromwellian Era Spy Message
The CRYPTOMATIC HC-520
Cryptographic Reflections on the Genetic Code
A Note on Public-Key Cryptosystems
Deciphered Texts--A Book Review
Memories of Friedman
Cryptanalysts' Corner
"Forwards and Backwards" Encryption
The Ciphering System for A 19th Century Challenge Cipher
Problems of the Unbreakable Cipher
Another Solution to the Sherlockian Cryptogram
The Market for Encryption
Reminiscences of a Master Cryptograph

Number 2

Interviews with Cryptologists
Applications of the Drazin Inverse to the Hill Cryptographic System I
A Curious Cryptic Composition
Some Cryptographic and Computing Applications of the Toshiba LC-836MN Memo Note 30 Pocket Calculator
Ready-made Love Letters
An Apology for Jacopo Silvestri
Memories of the Pacific--Book Reviews
Decryption of Simple Substitution Cyphers with Word Divisions Using a Content Addressable Memory
The Beale Cypher: A Dissenting Opinion
Nuggets from the Archive: A Null Code at the White House

Number 3

The Black Chamber: How the British Broke Enigma
High Speed Indirect Cryption
Finger Counting and the Identifications of James VI's Secret Agents
Applications of the Drazin Inverse to the Hill Cryptographic System II
Opportunities for the Amateur Cryptanalyst Can Be Anywhere
Spy Ciphers--A Book Review
Cryptanalysts' Corner
Cipher Devices: TRS-80 Data Privacy System
Linear Transformations in Galois Fields and Their Applications to Cryptography

Number 4

Some Special War Work--Part I
Remarks on Lu and Lee's Proposals for a Public-Key Cryptosystem
Cryptanalysts' Corner
Development of Commercial Cryptosystem Standards
Cipher Equipment: TST-1221
Transfinite Cryptography
Pearl Harbor Revisited--A Book Review
A Professional's Challenge
The Black Chamber: La Methodes des Batons
A Remarkable View of Ancient America--A Book Review
Results of Reader Survey

VOLUME 5 1981

Number 1

Graphic Solution of a Linear Transformation Cipher
The Public's Secrets
Statistical Analysis of the Hagelin Cryptograph
Some Special War Work--Part II
Cryptanalysts' Corner
The Black Chamber: Shutting Off
Equipment: Collins CR-200/220
Decrypting a Stream Cipher Based on J-K Flip Flops
From the Ultra Conference--A Book Review
A Theoretical Measure of Cryptographic Performance

Number 2

German Spy Cryptograms
Applications of the Drazin Inverse to the Hill Cryptographic System III
The Code-O-Graph Cipher Disks
The House Report on Public Cryptography
The Hand-Held Calculator as a Cryptographic Machine
The Public Cryptography Study Group
Cryptanalysts' Corner
A Code Problem--A Book Review

Number 3

Report of the Public Cryptography Study Group
Case against Restraints on Non-Governmental Research in Cryptography
Palatine and Bibliander on Ciphers
Reward for Reading and Deciphering--A Book Review
Measuring Cryptographic Performance with Production Processes
Sherlock Holmes in Babylon
Cipher Machine Exhibit at the Smithsonian Institution
The A-22 Cryptograph